United States Government Accountability Office

GAO

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

For release on delivery
expected at 10:00 a.m. EDT
May 11, 2011

INFORMATION TECHNOLOGY

Department of Veterans Affairs Faces Ongoing Management Challenges

Statement of Joel C. Willemssen,
Managing Director, Information Technology

GAO
Accountability * Integrity * Reliability

GAO-11-663T

GAO
Accountability • Integrity • Reliability

Highlights

Highlights from GAO-11-663T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, U.S. House of Representatives

May 11, 2011

INFORMATION TECHNOLOGY

Department of Veterans Affairs Faces Ongoing Management Challenges

Why GAO Did This Study

The use of information technology (IT) is crucial to helping the Department of Veterans Affairs (VA) effectively serve the nation's veterans, and the department has expended billions of dollars annually over the last several years to manage and secure its information systems and assets. VA has, however, experienced challenges in managing its IT. GAO has previously highlighted VA's weaknesses in managing and securing its information systems and assets.

GAO was asked to testify on its past work on VA's weaknesses in managing its IT resources, specifically in the areas of systems development, information security, and collaboration with the Department of Defense (DOD) on efforts to meet common health system needs.

What GAO Recommends

In previous reports in recent years, GAO has made numerous recommendations to VA aimed at improving the department's IT management capabilities. These recommendations were focused on: improving two projects to develop and implement new systems, strengthening information security practices and ensuring that security issues are adequately addressed, and overcoming barriers VA faces in collaborating with DOD to jointly address the departments' common health care business needs.

View GAO-11-663T or key components. For more information, contact Joel C Willemssen at (202) 512-6253 or willemssenj@gao.gov or Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov.

What GAO Found

Recently, GAO reported on two VA systems development projects that have yielded mixed results. For its outpatient appointment scheduling project, VA spent an estimated $127 million over 9 years and was unable to implement any of the planned capabilities. The application software project was hindered by weaknesses in several key management disciplines, including acquisition planning, requirements analysis, testing, progress reporting, risk management, and oversight. For its Post 9/11 GI Bill educational benefits system, VA used a new incremental software development approach and deployed the first two of four releases of its long-term system solution by its planned dates, thereby providing regional processing offices with key automated capabilities to prepare original and amended benefits claims. However, VA had areas for improvement, including establishing business priorities, testing the new systems, and providing oversight.

Effective information security controls are essential to securing the information systems and information on which VA depends to carry out its mission. For over a decade, VA has faced long-standing information security weaknesses as identified by GAO, VA's Office of the Inspector General, VA's independent auditor, and the department itself. The department continues to face challenges in maintaining its information security controls over its systems and in fully implementing the information security program required under the Federal Information Security Management Act of 2002. These weaknesses have left VA vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information.

VA and DOD operate two of the nation's largest health care systems, providing health care to 6 million veterans and 9.6 million active duty service members at estimated annual costs of about $48 billion and $49 billion, respectively. To provide this care, both departments rely on electronic health record systems to create, maintain, and manage patient health information. GAO reported earlier this year that VA faced barriers in establishing shared electronic health record capabilities with DOD in three key IT management areas—strategic planning, enterprise architecture (i.e., a description of business processes and supporting technologies), and IT investment management. Specifically, the departments were unable to articulate explicit plans, goals, and time frames for jointly addressing the health IT requirements common to both departments' electronic health record systems. Additionally, although VA and DOD took steps toward developing and maintaining artifacts related to a joint health architecture, the architecture was not sufficiently mature to guide the departments' joint health IT modernization efforts. Lastly, VA and DOD did not have a joint process for selecting IT investments based on criteria that consider cost, benefit, schedule, and risk elements, which would help to ensure that the chosen solution both meets the departments' common health IT needs and provides better value and benefits to the government as a whole. Subsequent to our report, the Secretaries of Veterans Affairs and Defense agreed to pursue integrated electronic health record capabilities.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be a part of today's dialogue with the subcommittee on the Department of Veterans Affairs' (VA) actions to better manage its information technology (IT) resources. The use of IT is crucial to helping VA effectively serve the nation's veterans and the department has expended billions of dollars over the last several years to manage and secure its information systems and assets—the department's budget for IT now exceeds $3 billion annually.

VA has, however, experienced challenges in managing its IT resources, as we have previously reported.[1] As you requested, in my testimony today, I will describe those challenges, specifically in the areas of systems development, information security, and collaborating with the Department of Defense (DOD) to jointly develop electronic health record system capabilities.

The information in my testimony is based primarily on our previous work at VA. We also obtained and analyzed pertinent documentation to determine the current status of selected department management efforts. We conducted our work in support of this testimony during May 2011 in the Washington, D.C., area. All work on which this testimony is based was conducted in accordance with generally accepted government auditing standards.

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

[1] GAO, *Electronic Health Records: DOD and VA Should Remove Barriers and Improve Efforts to Meet Their Common System Needs*, GAO-11-265 (Washington, D.C.: February 2011); *Information Technology: Veterans Affairs Can Further Improve Its Development Process for Its New Education Benefits System*, GAO-11-115 (Washington, D.C.: December 2010); *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, GAO-10-513 (Washington, D.C.: May 2010); *Information Technology: Management Improvements Are Essential to VA's Second Effort to Replace Its Outpatient Scheduling System*, GAO-10-579 (Washington, D.C.: May 2010); and *Information Security: Veterans Affairs Needs to Resolve Long-Standing Weaknesses*, GAO-10-727T (Washington, D.C.: May 19, 2010).

memorials. According to information from the department, its employees maintain the largest integrated health care system in the nation for more than 5 million patients at more than 1,500 sites of care, provide compensation and pension benefits for nearly 4 million veterans and beneficiaries, and maintain nearly 3 million gravesites at 163 properties. Over time, the use of IT has become increasingly important to the department's efforts to provide these benefits and services to veterans; VA relies on its IT systems for medical information and records and for processing benefits claims, including compensation and pension and education benefits. Further, VA is increasingly expected to improve its service to veterans by sharing information with other departments, especially DOD.

VA's fiscal year 2012 request for almost $3.2 billion in IT budget authority indicates the range of the department's IT activities. For example, the request includes:

- about $1.4 billion to operate and maintain existing infrastructure and systems;
- approximately $650 million to develop new system capabilities to support, for example, faster compensation and pension claims processing, elimination of veteran homelessness, and improvement of veteran mental health;
- $68 million for information security activities; and
- $915 million to fund about 7,000 IT personnel.

Our prior work has shown that success in managing IT depends, among other things, on having and using effective system development capabilities and having effective controls over information and systems. We have issued several products on VA in important management areas where the department faces challenges. My testimony today will briefly summarize these products.

Recent System Development Projects Have Achieved Varied Degrees of Success

Historically, VA has experienced significant IT development and delivery difficulties. We recently reported on two important VA systems development projects.[2] The first project expended an estimated $127 million without delivering any of the planned capabilities. VA has begun implementing capabilities from the second project, although we identified opportunities for improvement.

VA's Scheduling Replacement Project Was Hindered by Systems Development and Acquisition Weaknesses

To carry out VA's daily operations in providing care to veterans and their families, the department relies on an outpatient appointment scheduling system. However, according to the department, this current scheduling system has had long-standing limitations that have impeded its effectiveness. Consequently, VA began work on a replacement system in 2000. However, after spending an estimated $127 million over 9 years, VA had not implemented any of the planned capabilities.

VA's efforts to successfully complete the Scheduling Replacement Project were hindered by weaknesses in several key project management disciplines and a lack of effective oversight. Specifically,

- **VA did not adequately plan its acquisition of the scheduling application and did not obtain the benefits of competition.** The *Federal Acquisition Regulation* (FAR) required preparation of acquisition plans[3] that must address how competition will be sought, promoted, and sustained.[4] VA did not develop an acquisition plan until May 2005, about 4 years after the department first contracted

[2] GAO-10-579 and GAO-11-115.

[3] See FAR, subpart 7.1. See also FAR 34.004.

[4] See FAR 7.105 b(2).

for a new scheduling system. Further, VA did not promote competition in contracting for its scheduling system. Instead, VA issued task orders against an existing contract that the department had in place for acquiring services such as printing, computer maintenance, and data entry. These weaknesses in VA's acquisition management reflected the inexperience of the department's personnel in administering major IT contracts. To address identified shortcomings, we recommended that VA ensure that future acquisition plans document how competition will be sought, promoted, and sustained.

- **VA did not ensure that requirements were complete and sufficiently detailed.** Effective, disciplined practices for defining requirements include analyzing requirements to ensure that they are complete, verifiable, and sufficiently detailed.[5] For example, maintaining bidirectional traceability from high-level operational requirements through detailed low-level requirements to test cases is a disciplined requirements management practice. However, VA did not adequately define requirements. For example, in November 2007, VA determined that performance requirements were missing and that some requirements were not testable. Further, according to project officials, some requirements were vague and open to interpretation. Also, requirements for processing information from other systems were missing. The incomplete and insufficiently detailed requirements resulted in a system that did not function as intended. In addition, VA did not ensure that requirements were fully traceable. As early as October 2006, an internal review noted that the requirements did not trace to business rules or to test cases. By not ensuring requirements traceability, the department increased the risk that the system could not be adequately tested and would not function as intended. We therefore recommended that VA ensure implementation of a requirements management plan that reflected leading practices.

[5] See Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Development*, *version 1.2* (Pittsburgh, Pa., August 2006), and *Software Acquisition Capability Maturity Model (SA-CMM) version 1.03*, CMU/SEI-2002-TR-010 (Pittsburgh, Pa., March 2002).

- **VA's concurrent approach to performing system tests increased risk.** Best practices in system testing indicate that testing activities should be performed incrementally, so that problems and defects[6] with software versions can be discovered and corrected early. VA's guidance on conducting tests is consistent with these practices and specifies four test stages and associated criteria for progressing through the stages.[7] For example, defects categorized as critical, major, and average severity identified in testing stage one are to be resolved before testing in stage two is begun. Nonetheless, VA took a high-risk approach to testing by performing tests concurrently rather than incrementally. Scheduling project officials told us that they ignored their own testing guidance and performed concurrent testing at the direction of Office of Enterprise Development senior management in an effort to prevent project timelines from slipping. The first version to undergo stage two testing had 370 defects that should have been resolved before stage two testing was begun. Almost 2 years after beginning stage two testing, 87 defects that should have been resolved before stage two testing began had not been fixed. As a result of a large number of defects that VA and the contractor could not resolve, the contract was terminated. To prevent these types of problems with future system development efforts, we recommended that VA adhere to its own guidance for system testing.

- **VA's reporting based on earned value management data was unreliable.** The Office of Management and Budget (OMB) and VA policies require major projects to use earned value management[8] to measure and report progress. Earned value management is a tool for measuring a project's progress by comparing the value of work accomplished with the amount of work expected to be

[6] Defects are system problems that require a resolution and can be due to a failure to meet the system specifications.

[7] According to VA testing documentation, these stages are (1) testing within the VA development team, (2) testing services, (3) field testing, and (4) final review and acceptance testing.

[8] OMB issued policy guidance (M-05-23) to agency CIOs on improving technology projects that includes requirements for reporting performance to OMB using earned value management (August 2005).

accomplished. Such a comparison permits actual performance to be evaluated and is based on variances[9] from the cost and schedule baselines. In January 2006, the scheduling project began providing monthly reports to the department's Chief Information Officer based on earned value management data. However, the progress reports included contradictory information about project performance. Specifically, the reports featured stoplight indicators (green, yellow, or red) that frequently were inconsistent with the reports' narrative. For example, the June 2007 report identified project cost and schedule performance as green, despite the report noting that the project budget was being increased by $3 million to accommodate schedule delays. This inconsistent reporting continued until October 2008, when the report began to show cost and schedule performance as red, the actual state of the project. Further, the former program manager noted that the department performed earned value management for the scheduling project only to fulfill the OMB requirement, and that the data were not used as the basis for decision making because doing so was not a part of the department's culture. To address these weaknesses, we recommended that VA ensure effective implementation of earned value management.

- **VA did not effectively identify, mitigate, and communicate project risks.** Federal guidance and best practices advocate risk management.[10] To be effective, risk management activities should include identifying and prioritizing risks as to their probability of occurrence and impact, documenting them in an inventory, and developing and implementing appropriate risk mitigation strategies. VA established a process for managing the scheduling system project's risks that was consistent with relevant best practices.

[9] Cost variances compare the value of the completed work (i.e., the earned value) with the actual cost of the work performed. Schedule variances are also measured in dollars, but they compare the earned value of the completed work with the value of the work that was expected to be completed. Positive variances indicate that activities cost less or are completed ahead of schedule. Negative variances indicate activities cost more or are falling behind schedule.

[10] OMB Circular A-130 (Nov. 30, 2000) and Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration for Development*, version 1.2 (Pittsburgh, Pa., August 2006).

Specifically, project officials developed a risk management plan that defined five phases—risk identification, risk analysis, risk response planning, risk monitoring and control, and risk review. However, the department did not take key project risks into account. Senior project officials indicated that staff members were often reluctant to raise risks or issues to leadership due to the emphasis on keeping the project on schedule. Accordingly, VA did not identify as risks (1) using a noncompetitive acquisition approach, (2) conducting concurrent testing and initiation of stage two testing with significant defects, and (3) reporting unreliable project cost and schedule performance information. Any one of these risks alone had the potential to adversely impact the outcome of the project. The three of them together dramatically increased the likelihood that the project would not succeed. To improve management of the project moving forward, we recommended that VA identify risks related to the scheduling project and prepare plans and strategies to mitigate them.

- **VA's oversight boards did not take corrective actions despite the department becoming aware of significant issues.** GAO and OMB guidance call for the use of institutional management processes to control and oversee IT investments.[11] Critical to these processes are milestone reviews that include mechanisms to identify underperforming projects, so that timely steps can be taken to address deficiencies. These reviews should be conducted by a department-level investment review board composed of senior executives. In this regard, VA's Enterprise Information Board was established to provide oversight of IT projects through in-process reviews when projects experience problems. Similarly, the Programming and Long-Term Issues Board is responsible for performing milestone reviews and program management reviews of projects. However, between June 2006 and May 2008, the department did not provide oversight of the Scheduling Replacement Project, even though the department had become

[11] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004) and OMB, *Capital Programming Guide: Supplement to Circular A-11, Part 7, Planning, Budgeting, and Acquisition of Capital Assets* (Washington, D.C., June 2006).

aware that the project was having difficulty meeting its schedule and performance goals. According to the chairman of the Programming and Long-Term Issues Board, it did not conduct reviews of the scheduling project prior to June 2008 because it was focused on developing the department's IT budget strategy. To address these deficiencies, in June 2009, VA began establishing the Program Management Accountability System to promote visibility into troubled programs and allow the department to take corrective actions. We recommended that VA ensure the policies and procedures it was establishing were executed effectively.

In response to our report, VA concurred with our recommendations and described its actions to address them. For example, the department stated that it would work closely with contracting officers to ensure future acquisition plans clearly identify an acquisition strategy that promotes full and open competition. In addition, the department stated that the Program Management Accountability System will provide near-term visibility into troubled programs, allowing the Principal Deputy Assistant Secretary for Information and Technology to provide help earlier and avoid long-term project failures.

In May 2011, VA's program manager stated that the department's effort to develop a new outpatient scheduling system—now referred to as 21st Century Medical Scheduling—consists largely of planning activities, including the identification of requirements. However, according to the manager, the project is not included in the department's fiscal year 2012 budget request. As a result, the department's plans for addressing the limitations that it had identified in its current scheduling system are uncertain.

VA Has Partially Delivered New Education Benefits System Capabilities, but Can Improve Its Development Process

In contrast to the scheduling system project failure, VA has begun implementing a new system for processing a recently established education benefit for veterans. The Post-9/11 GI Bill provides educational assistance for veterans and members of the armed forces who served on or after September 11, 2001. VA concluded that its existing system and manual processes were insufficient to

support the new benefits. For instance, the system was not fully integrated with other information systems such as VA's payments system, requiring claims examiners to access as many as six different systems and manually input claims data. Consequently, claims examiners reportedly took up to six times longer to pay Post-9/11 GI Bill program claims than other VA education benefit claims. The challenges associated with its processing system contributed to a backlog of 51,000 claims in December 2009. In response to this situation, the department began an initiative to modernize its benefits processing capabilities. VA chose an incremental development approach, referred to as Agile software development,[12] which is intended to deliver functionality in short increments before the system is fully deployed.

In December 2010, we reported that VA had delivered key automated capabilities used to process the new education benefits. Specifically, it deployed the first two of four releases of its long-term system solution by its planned dates, thereby providing regional processing offices with key automated capabilities to prepare original and amended benefits claims. Further, VA established Agile practices including a cross-functional team that involves senior management, governance boards, key stakeholders, and distinct Agile roles and began using three other Agile practices—focusing on business priorities, delivering functionality in short increments, and inspecting and adapting the project.

However, to help guide the full development and implementation of the new system, we reported that VA could make further improvements to these practices in five areas.

1. **Business priorities.** To ensure business priorities are a focus, a project starts with a vision that contains, among other things, a purpose, goals, metrics, and constraints. In addition, it should be traceable to requirements. VA established a vision that captured

[12]Agile software development is not a set of tools or a single methodology, but a philosophy based on selected values, such as, the highest priority is to satisfy customers through early and continuous delivery of valuable software; delivering working software frequently, from a couple of weeks to a couple of months; and that working software is the primary measure of progress. For more information on Agile development, see http://www.agilealliance.org.

the project purpose and goals; however, it had not established metrics for the project's goals or prioritized project constraints. Department officials stated that project documentation was evolving and they intended to improve their processes based on lessons learned; however, until it identified metrics and constraints, the department did not have the means to compare the projected performance with the actual results. We recommended that VA establish performance measures for goals and identify constraints to provide better clarity in the vision and expectations of the project.

2. **Traceability.** VA had also established a plan that identified how to maintain requirements traceability within an Agile environment; however, the traceability was not always maintained between legislation, policy, business rules, and test cases. We recommended that VA establish bidirectional traceability between requirements and legislation, policies, and business rules.

3. **Definition of "done."** To aid in delivering functionality in short increments, defining what constitutes completed work and testing functionality is critical.[13] However, VA had not established criteria for work that was considered "done" at all levels of the project. Program officials stated that each development team had its own definition of "done" and agreed that they needed to provide a standard definition across all teams. Without a mutual agreement for what constitutes "done" at each level, the resulting confusion can lead to inconsistent quality. We therefore recommended that VA define the conditions that must be present to consider work "done" in adherence with agency policy and guidance.

4. **Testing.** While the department had established an incremental testing approach, the quality of unit and functional testing

[13] One of the key Agile principles is that the delivery of completed software be defined, commonly referred to as the definition of "done." This is critical to the development process to help ensure that, among other things, testing has been adequately performed and the required documentation has been developed.

performed during Release 2 was inadequate in 10 of the 20 segments of system functionality we reviewed. Program officials stated that they placed higher priority on user acceptance testing at the end of a release and relied on users to identify defects that were not detected during unit and functional testing. Without improved testing quality, the department risks deploying future releases that contain defects that may require rework. To reduce defects and rework to fix them, we recommended that VA improve the adequacy of the unit and functional testing processes.

5. **Oversight.** In order for projects to be effectively inspected and adapted, management must have tools to provide effective oversight. For Agile development, progress and the amount of work remaining can be reflected in a burn-down chart, which depicts how factors such as the rate at which work is completed (velocity) and changes in overall product scope affect the project over time. While VA had an oversight tool that showed the percentage of work completed to reflect project status at the end of each iteration, it did not depict the velocity of the work completed and the changes to scope over time. We therefore recommended that VA implement an oversight tool to clearly communicate velocity and the changes to project scope over time.

VA concurred with three of our five recommendations. It did not concur with our recommendation that it implement an oversight tool to clearly communicate velocity. However, without this level of visibility in its reporting, management and the development teams may not have all the information they need to fully understand project status. VA also did not concur with our recommendation to improve the adequacy of the unit and functional testing processes to reduce the amount of system rework. However, without increased focus on the quality of testing early in the development process, VA risks delaying functionality and/or deploying functionality with unknown defects that could require future rework that may be costly and ultimately impede the claims examiners' ability to process claims efficiently.

In early May 2011, we reported that the implementation of remaining capabilities is behind schedule and additional modifications are needed.[14] According to VA officials, system enhancements such as automatic verification of the length of service were delayed because of complexities with systems integration and converting data from the interim system. Additionally, recent legislative changes to the program required VA to modify the system and its deployment schedule. For instance, VA will need to modify its system to reflect changes to the way tuition and fees are calculated—an enhancement that officials described as difficult to implement. Because of these delays, final deployment of the system is now scheduled for the end of 2011—a year later than planned.

VA Continues to Face Information Security Challenges

Effective information security controls[15] are essential to securing the information systems and information on which VA depends to carry out its mission. Without proper safeguards, the department's systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The consequence of weak information security controls was illustrated by VA's May 2006 announcement that computer equipment containing personal information on veterans and active duty military personnel had been stolen. Further, over the last few years, VA has reported an increasing number of security incidents and events. Specifically, each year during fiscal years 2007 through 2009, the department

[14] GAO, *Veterans' Education Benefits: Enhanced Guidance and Collaboration Could Improve Administration of the Post-9/11 GI Bill Program*, GAO-11-356R (Washington, D.C.: May 2011).

[15] Information system general controls affect the overall effectiveness and security of computer operations and are not unique to specific computer applications. These controls include security management, configuration management, operating procedures, software security features, and physical protections designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that incompatible computer-related duties are segregated, and that backup and recovery plans are adequate to ensure the continuity of operations.

reported a higher number of incidents and the highest number of incidents in comparison to 23 other major federal agencies.

To help protect against threats to federal systems, the Federal Information Security Management Act of 2002 (FISMA) sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The framework creates a cycle of risk management activities necessary for an effective security program. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to OMB, agency heads, chief information officers, inspectors general, and the National Institute of Standards and Technology (NIST), in particular requiring chief information officers and inspectors general to submit annual reports to OMB.

In addition, Congress enacted the Veterans Benefits, Health Care, and Information Technology Act of 2006.[16] Under the act, VA's Chief Information Officer is responsible for establishing, maintaining, and monitoring departmentwide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program. It also reinforced the need for VA to establish and carry out the responsibilities outlined in FISMA, and included provisions to further protect veterans and service members from the misuse of their sensitive personal information and to inform Congress regarding security incidents involving the loss of that information.

Weaknesses in Security Controls Have Placed VA's Systems at Risk

Information security has been a long-standing challenge for the department, as we have previously reported. In 2010, for the 14th year in a row, VA's independent auditor reported that inadequate information system controls over financial systems constituted a

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

material weakness.[17] Among 24 major federal agencies, VA was one of eight agencies in fiscal year 2010 to report such a material weakness.

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

- Passwords for key VA network domains and financial applications were not consistently configured to comply with agency policy.
- Testing of contingency plans for financial management systems at selected facilities was not routinely performed and documented to meet the requirements of VA policy.
- Many IT security control deficiencies were not analyzed and remediated across the agency and a large backlog of deficiencies remained in the VA plan of action and milestones system. In addition, previous plans of action and milestones were closed without sufficient and documented support for the closure.

In addition, VA has consistently had weaknesses in major information security control areas. As shown in table 1, for fiscal years 2007 through 2010, deficiencies were reported in each of the five major categories of information security access controls[18] as

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

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

defined in our *Federal Information System Controls Audit Manual.*[19]

Table 1: Control Weaknesses for Fiscal Years 2007 - 2010

Security control category	2007	2008	2009	2010
Access control	•	•	•	•
Configuration management	•	•	•	•
Segregation of duties	•	•	•	•
Contingency planning	•	•	•	•
Security management	•	•	•	•

Source: GAO analysis based on VA and Inspector General reports.

In fiscal year 2010, for the 11th year in a row, the VA's Office of Inspector General designated VA's information security program and system security controls as a major management challenge for the department. Of 24 major federal agencies, the department was 1 of 23 to have information security designated as a major management challenge. The Office of Inspector General noted that the department had made progress in implementing components of an agencywide information security program, but nevertheless continued to identify major IT security deficiencies in the annual information security program audits. To assist the department in improving its information security, the Office of Inspector General made recommendations for strengthening access controls, configuration management, change management, and service continuity. Effective implementation of these recommendations could help VA to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data.

In March 2010, we reported[20] that federal agencies, including VA, had made limited progress in implementing the Federal Desktop Core Configuration (FDCC) initiative to standardize settings on

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

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

workstations.[21] We determined that VA had implemented certain requirements of the initiative, such as documenting deviations from the standardized set of configuration settings for Windows workstations and putting a policy in place to officially approve these deviations. However, VA had not fully implemented several key requirements. For example, the department had not included language in contracts to ensure that new acquisitions address the settings and that products of IT providers operate effectively using them. Additionally, VA had not obtained a NIST-validated tool to monitor implementation of standardized workstation configuration settings. To improve the department's implementation of the initiative, we made four recommendations: (1) complete implementation of VA's baseline set of configuration settings, (2) acquire and deploy a tool to monitor compliance with FDCC, (3) develop, document, and implement a policy to monitor compliance, and (4) ensure that FDCC settings are included in new acquisitions and that products operate effectively using these settings. VA concurred and has addressed the recommendation to ensure settings are included in new acquisitions. The department intends to implement the remaining recommendations in the future.

VA's Uneven Implementation of FISMA Has Limited the Effectiveness of Security Efforts

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

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

- employees and contractors receiving IT security awareness training and those who have significant security responsibilities and have received specialized security training,
- systems whose controls were tested and evaluated, have tested contingency plans, and are certified and accredited.[22]

Since fiscal year 2006, VA's progress in fully implementing the information security program required under FISMA and following the policies issued by OMB has been mixed. For example, from 2006 to 2009, the department reported a dramatic increase in the percentage of systems for which a contingency plan was tested in accordance with OMB policy. However, during the same period, it reported decreases in both the percentage of employees who had received security awareness training and the percentage of employees with significant security responsibilities who had received specialized security training. These decreases in the percentage of individuals who had received information security training could limit the ability of VA to effectively implement security measures.

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

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

and lower percentages of individuals with significant security responsibilities who received specialized security training.

Cloud Computing Presents Opportunities but Poses IT Security Challenges

Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers, while freeing them from the burden and costs of maintaining the underlying infrastructure. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. The President's budget has identified the adoption of cloud computing in the federal government as a way to more efficiently use the billions of dollars spent annually on IT. However, as we reported in May 2010,[23] federal guidance and processes that specifically address information security for cloud computing had not yet been developed, and those cloud computing programs that have been implemented may not have effective information security controls in place.

As we reported, cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include dependence on the security practices and assurances of the provider, dependence on the provider, and concerns related to sharing computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation. We made recommendations to OMB, the General Services Administration, and NIST to assist agencies in identifying uses of cloud computing and necessary security measures, selecting and acquiring cloud computing products and services, and implementing appropriate information security controls when using cloud computing.

[23] GAO-10-513.

VA Faces Barriers to Establishing Shared Electronic Health Record Capabilities with DOD

VA and DOD have two of the nation's largest health care operations, providing health care to 6 million veterans and 9.6 million active duty service members and their beneficiaries at estimated annual costs of about $48 billion and $49 billion, respectively. Although the results of a 2008 study found that more than 97 percent of functional requirements for an inpatient electronic health record system are common to both departments, the departments have spent large sums of money to separately develop and operate electronic health record systems. Furthermore, the departments have each begun multimillion dollar modernizations of their electronic health record systems. Specifically, VA reported spending almost $600 million from 2001 to 2007 on eight projects as part of its Veterans Health Information Systems and Technology Architecture (VistA) modernization. In April 2008, VA estimated an $11 billion total cost to complete the modernization by 2018. For its part, DOD has obligated approximately $2 billion over the 13-year life of its Armed Forces Health Longitudinal Technology Application (AHLTA) and requested $302 million in fiscal year 2011 funds for a new system.

Additionally, VA and DOD are working to establish the Virtual Lifetime Electronic Record (VLER), which is intended to facilitate the sharing of electronic medical, benefits, and administrative information between the departments. VLER is further intended to expand the departments' health information sharing capabilities by enabling access to private sector health data. The departments are also developing joint IT capabilities for the James A. Lovell Federal Health Care Center (FHCC) in North Chicago, Illinois. The FHCC is to be the first VA/DOD medical facility operated under a single line of authority to manage and deliver medical and dental care for veterans, new Naval recruits, active duty military personnel, retirees, and dependents.

In February 2011, we reported that VA and DOD lacked mechanisms for identifying and implementing efficient and effective IT solutions to jointly address their common health care system needs as a result

of barriers in three key IT management areas—strategic planning, enterprise architecture, and investment management.

- **Strategic planning:** The departments were unable to articulate explicit plans, goals, and time frames for jointly addressing the health IT requirements common to both departments' electronic health record systems. For example, VA's and DOD's joint strategic plan did not discuss how or when the departments propose to identify and develop joint health IT solutions, and department officials did not determine whether the IT capabilities developed for the FHCC could or would be implemented at other VA and DOD medical facilities.

- **Enterprise architecture:** Although VA and DOD had taken steps toward developing and maintaining artifacts related to a joint health architecture (i.e., a description of business processes and supporting technologies), the architecture was not sufficiently mature to guide the departments' joint health IT modernization efforts. For example, the departments did not define how they intended to transition from their current architecture to a planned future state.

- **Investment management:** VA and DOD did not establish a joint process for selecting IT investments based on criteria that consider cost, benefit, schedule, and risk elements, which would help to ensure that a chosen solution both meets the departments' common health IT needs and provides better value and benefits to the government as a whole.

These barriers resulted in part from VA's and DOD's decision to focus on developing VLER, modernizing their separate electronic health record systems, and developing IT capabilities for FHCC, rather than determining the most efficient and effective approach to jointly addressing their common requirements. Because VA and DOD continued to pursue their existing health information sharing efforts without fully establishing the key IT management capabilities described, they may have missed opportunities to successfully deploy joint solutions to address their common health care business needs.

VA's and DOD's experiences in developing VLER and IT capabilities for FHCC offered important lessons to improve the departments' management of these ongoing efforts. Specifically, the departments can improve the likelihood of successfully meeting their goal to implement VLER nationwide by the end of 2012 by developing an approved plan that is consistent with effective IT project management principles. Also, VA and DOD can improve their continuing effort to develop and implement new IT system capabilities for FHCC by developing a plan that defines the project's scope, estimated cost, and schedule in accordance with established best practices. Unless VA and DOD address these lessons, the departments will jeopardize their ability to deliver expected capabilities to support their joint health IT needs.

We recommended several actions that the Secretaries of Veterans Affairs and Defense could take to overcome barriers that the departments face in modernizing their electronic health record systems to jointly address their common health care business needs, including the following:

- Revise the departments' joint strategic plan to include information discussing their electronic health record system modernization efforts and how those efforts will address the departments' common health care business needs.
- Further develop the departments' joint health architecture to include their planned future state and transition plan from their current state to the next generation of electronic health record capabilities.
- Define and implement a process, including criteria that considers costs, benefits, schedule, and risks, for identifying and selecting joint IT investments to meet the departments' common health care business needs.

We also recommended that the Secretaries of Veterans Affairs and Defense strengthen their ongoing efforts to establish VLER and the joint IT system capabilities for FHCC by developing plans that include scope definition, cost and schedule estimation, and project plan documentation and approval.

Both departments concurred with our recommendations and on March 17, 2011, the Secretaries of Veterans Affairs and Defense committed their respective departments to pursue joint development and acquisition of integrated electronic health record capabilities.

In summary, effective IT management is critical to the performance of VA's mission. However, the department faces challenges in key areas, including systems development, information security, and collaboration with DOD. Until VA fully addresses these and implements key recommendations, the department will likely continue to (1) deliver system capabilities later than expected; (2) expose its computer systems and sensitive information (including personal information of veterans and their beneficiaries) to an unnecessary and increased risk of unauthorized use, disclosure, tampering, theft, and destruction; and (3) not provide efficient and effective joint DOD/VA solutions to meet the needs of our nation's veterans.

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

Contacts and Acknowledgments

If you have questions concerning this statement, please contact Joel C. Willemssen, Managing Director, Information Technology Team, at (202) 512-6253 or willemssenj@gao.gov; or Valerie C. Melvin, Director, Information Management and Human Capital Issues, at (202) 512-6304 or melvinv@gao.gov. Other individuals who made key contributions include Mark Bird, Assistant Director; Mike Alexander; Nancy Glover; Paul Middleton; and Glenn Spiegel.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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