United States General Accounting Office

GAO

Testimony

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

**For Release on Delivery**
**Expected at**
**10 a.m. EDT**
**Wednesday,**
**April 4, 2001**

# VA INFORMATION TECHNOLOGY

# Important Initiatives Begun, Yet Serious Vulnerabilities Persist

Statement of David L. McClure
Director, Information Technology Management Issues

GAO-01-550T

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to join in today's hearing and share updated information on the Department of Veterans Affairs' (VA) information technology (IT) program. As you know, IT is essential to VA's ability to effectively serve the veteran population and is the cornerstone of the department's "One VA" vision of providing seamless services to veterans and their families.

Over the past 5 years, VA has spent about $1 billion each year in support of its IT program, and it expects its IT expenditures to continue increasing over the next 5 years—from about $1.4 billion in fiscal year 2001 to more than $2.1 billion by fiscal year 2005. Yet, as we have testified and reported in the past,[1] the department has encountered numerous and consistent challenges associated with managing IT, including weaknesses in its processes for selecting, controlling, and evaluating investments; the absence of a departmentwide enterprise architecture; and ineffective computer security management.

At your request, we have conducted work to review the status of VA's efforts to continue to improve its overall IT management in response to concerns raised by our past reviews. In my remarks today, I will discuss VA's actions to

- fill its chief information officer (CIO) position;
- improve computer security, including securing its on-line compensation and pension applications;
- improve its processes for selecting, controlling, and evaluating IT investments;
- complete an enterprise architecture; and
- utilize the Veterans Health Administration's (VHA) Decision Support System and implement the Veterans Benefits Administration's (VBA) compensation and pension replacement project.

---

[1] *VA Information Technology: Progress Continues Although Vulnerabilities Remain* (GAO/T-AIMD-00-321, September 21, 2000); *Information Technology: VA Actions Needed to Implement Critical Reforms* (GAO/AIMD-00-226, August 16, 2000*); Information Technology: Update on VA Actions to Implement Critical Reform*s (GAO/T-AIMD-00-74, May 11, 2000); *VA Information Technology: Improvements Needed to Implement Legislative Reforms* (GAO/AIMD-98-154, July 7, 1998).

Collectively, these areas represent critically important challenges that VA needs to fully address if it is to successfully fulfill its goal of improving service delivery to veterans through the use of information technology.

## RESULTS IN BRIEF

VA is continuing to make progress in improving its overall IT management; however, important actions in several areas remain incomplete and require continued attention and decisions from the department's executive management. To begin with, the department has yet to fill the position of assistant secretary for information and technology, created in June 1998 and intended to serve as VA's chief information officer (CIO). It is critical that the department fill this leadership position to help the Secretary's executive management team fully address VA's critical IT challenges and achieve improvements in investment results that support the department's programs and operations.

In the area of computer security, VA has established a department-level information security management program and developed an information security management plan that addresses many of the security concerns that we and VA's Inspector General have identified. In addition, the department has recently hired a senior executive for computer security to demonstrate its commitment to this crucial area. The department has also done a good job in developing and posting privacy and security statements for its primary and secondary Web sites that are consistent with OMB requirements.

However, we remain concerned about the lack of adequate department policy and guidance for security, vulnerability and risk assessments, assessments or reports of threats and incidents, and comprehensive coordinating and monitoring responsibilities for its central security management group. For example, while VBA's Veterans On-Line Application demonstrates attention to short-term security problems we have identified in the past—such as stronger application access and personnel controls—it remains vulnerable to continuing weaknesses in VBA's networks and general support systems. Further, despite strong privacy policy statement postings on its Web sites, we discovered two Web pages that were using persistent "cookies"—a short string of text

sent from a Web server to a Web browser that is often used to recognize returning users and track Web browsing behavior—despite OMB policies limiting their use.

Moreover, VA continues to show progress in improving its guidance used to manage its investments in information technology. However, more concerted actions and discipline are needed to enforce this decisionmaking process, particularly in regard to consistent and complete tracking of IT cost data and critical in-process and post-implementation reviews of projects funded with its existing $1.4-billion annual IT budget. In addition, the department has not yet developed the integrated, departmentwide enterprise architecture needed to acquire and utilize information systems across VA in a cost-effective and efficient manner.

Lastly, two highly visible projects in the department's IT investment portfolio--VHA's Decision Support System (DSS) and VBA's compensation and pension (C&P) replacement project show progress. However, this latter project has not been fully implemented and both projects face managerial challenges related to their full and successful utilization. Some VHA medical centers and Veterans Integrated Service Networks (VISN) report greater use and specific clinical decisionmaking and resource allocation benefits from DSS usage. Clear top management expectations for its use in the centers and the assignment of staff knowledgeable in the use of the application are cited as important factors for higher use levels. Similarly, VBA's C&P replacement project is benefiting from greater project management attention; a limited pilot test was conducted in February 2001, with no reported problems. However, VBA will continue to face challenges as it attempts to move forward from its pilot to full-scale operational implementation.

## APPOINTMENT OF A CHIEF INFORMATION OFFICER IS CRITICAL TO THE SUCCESS OF VA's IT PROGRAM

Successful implementation of VA's IT program requires strong leadership and management to help define and guide the department's plans and actions. The Clinger-Cohen Act, passed in 1996,[2] directs the heads of major federal agencies to appoint CIOs to promote improvements in

[2]P.L. 104-106, Division E.

their agencies' work processes; implement integrated agencywide architectures; and help establish sound investment review processes to select, control, and evaluate IT spending.

In September 2000,[3] we testified about actions VA has taken over the last 3 years toward establishing the CIO position, including separating the CIO function from that of the chief financial officer, and establishing the position of assistant secretary for information and technology to serve as the department-level CIO. To his credit, the newly appointed Secretary of Veterans Affairs has identified filling the department's CIO position as one of his top priorities, and is currently conducting an extensive search to identify suitable candidates for the position, which requires Senate confirmation.

Our recently issued research report on the effective use of CIOs in several leading private and public organizations[4] provides insight into factors contributing to CIO successes. Three key principles stood out:

> First, senior executives must embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making. Specifically, the type of CIO chosen is matched to the organizations' needs. Most important, the top executives of these organizations determined how a CIO would best fit within existing or new management tiers to guide technology solutions.
>
> Second, effective CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. While placement of the CIO position at an executive management level in the organization is important, effective CIOs earned credibility and produced results by establishing effective working relationships with business unit heads.
>
> Third, CIOs must structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy

[3] GAO/T-AIMD-00-321, September 21, 2000.
[4] *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations* GAO-01-376G, February 2001).

structures, and available IT skills, this understanding is necessary to ensure that the CIO's office is aligned to best serve the needs of the enterprise.

Despite its creation in 1998 and the current recruitment effort by the Secretary, VA still does not have a person appointed as the departmentwide CIO. Instead, various VA officials have served as acting CIOs for the department during this time. The department's eventual CIO appointee faces challenges that will be difficult to resolve without constant support and involvement of VA's top executives. Under current arrangements, IT systems and services are highly decentralized among VA's administrations and staff offices. Out of VA's approximately $1.4 billion fiscal year 2001 IT budget, VHA oversees approximately $762.7 million, VBA approximately $79.5 million, and the National Cemetery Administration (NCA) approximately $0.4 million.[5] With such a large annual funding base and a decentralized IT management structure, it is crucial that the CIO ensure that well-established and integrated processes for leading, managing, and controlling IT investments are commonplace and followed throughout the department.

## INFORMATION SECURITY AND PRIVACY CHALLENGES REMAIN

As you know, computer security is critical to VA's ability to safeguard its assets, maintain the confidentiality of sensitive information, and ensure the reliability of its financial data. If effective computer security practices are not in place, financial and sensitive information contained in VA's systems are at risk of inadvertent or deliberate misuse, fraud, improper disclosure, or destruction—possibly occurring without detection. Likewise, as VA continues to expand its use of Web-based electronic services for interacting with and providing services to veterans, ensuring privacy of sensitive records containing personal information becomes essential.

[5] The remaining $589 million is for VA-wide initiatives in the financial management, human resources, infrastructure, security, architecture, and planning areas.

Steps Taken to Continue to Address
Recognized Security Weaknesses

Over the past several years, we have issued numerous reports and testimonies on VA's computer security weaknesses. Most recently, in September 2000, we reported[6] and testified[7] that serious computer security problems persisted throughout VHA and the department because VA had not fully implemented an integrated security management program and VHA had not effectively managed computer security at its medical facilities. Consequently, financial transaction data and personal information on veterans' medical records continued to face increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. We recommended that the department develop computer security guidance and oversight processes, and monitor and resolve coordination issues that could affect the success of the departmentwide computer security program.

VA concurred with our recommendations and continues to take constructive steps to address them. Specifically, it has now established a department-level information security management program and hired an executive-level official to head it. In addition, in November 2000, it finalized an information security management plan that provides a framework for addressing departmentwide information security on a near- and long-term basis. The plan addresses some of the longstanding departmentwide security problems that we, VA's Office of Inspector General, and the department's own internal reviews have identified. The plan also responds to risks documented in a departmentwide risk assessment that VA completed in June 2000, by recommending specific controls to reduce several vulnerabilities.

Additionally, VA's information security management plan emphasizes an accelerated (near-term), enterprisewide improvement of information security that is directed primarily at improving access and personnel controls. The plan identifies eight near-term actions that are to be completed between December 1, 2000 and May 1, 2001, including (1) implementing stronger

[6] *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration* (GAO/AIMD-00-232, September 8, 2000).
[7] GAO/T-AIMD-00-321, September 21, 2000.

passwords on computer workstations, (2) removing unsecured dial-in connections, and (3) conducting focused reviews of access and personnel controls.

VA's plan also identified a number of long-term actions emphasizing broader assessments and proposed measures to improve information security on a more comprehensive basis. These actions, which are to be implemented between July 1, 2001 and January 1, 2003, include proposals for establishing a regular cycle to test the department's compliance with established security requirements, and provisions for certifying and accrediting general support systems and major applications, as required by OMB Circular A-130.

## A Stronger Management Focus Is Needed to Resolve Lingering Departmentwide Security Problems

The success of VA's computer security management program is largely contingent upon how effectively the department manages risks to business operations that rely on its automated and highly interconnected systems. In our 1998 report on effective security practices used by several leading public and private organizations[8] and a companion report on risk-based security approaches in November 1999,[9] we identified key principles that can be used to establish a management framework for more effective information security programs. In our study, we found that the leading organizations we examined applied these principles to ensure that information security addressed risks on an ongoing basis. These have been cited as useful guidance for agencies by the federal CIO Council and incorporated into the Council's recently issued Information Security Assessment Framework, intended for agency self-assessments.[10]

A contributing factor to VA's continuing information security problems is that the department has not yet implemented key components of a comprehensive, integrated security management program. We brought many of these components to the department's attention last September.[11] Establishing its central security group, hiring a new information security executive who will

[8] *Information Security Management: Learning from Leading Organizations* (GAO/AIMD-98-68, May 1998).
[9] *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).
[10] *Federal Information Technology Security Assessment Framework,* November 28, 2000.
[11] GAO/AIMD-00-232, September 8, 2000.

report to the CIO, and partially implementing its security program plan are positive steps forward, but several critical actions related to our past recommendations and leading security management principles mentioned above require additional work and senior management attention. Let me briefly discuss four specific areas:

*Security Policy, Procedures, and Guidance.* Up-to-date, comprehensive, and well-communicated information security policies and implementation guidance serve as the foundation for effective information security programs and form the basis for adopting specific procedures and technical controls.[12] However, VA's information security management plan does not include steps for ensuring that policies and procedural guidelines adequately address the security of the department's interconnected computer environment, or that they cover other key security management areas, such as risk identification and categorization. Further, the plan does not include any provisions for developing technical security standards for system and security software. By setting technical security standards for system and security software and routinely evaluating the technical implementation of these standards, VA could eliminate or mitigate security exposure that we previously reported in these areas.

*Development of Risk-Based Security Assessments.* Our study of computer security best practices found that procedures for conducting risk assessments generally specified (1) how risk assessments should be initiated and conducted, (2) who should participate in the risk assessment, (3) how disagreements should be resolved, (4) what approvals were needed, and (5) how assessments should be documented and maintained. However, VA's information security management plan does not include a requirement for developing policy and guidance related to performing risk assessments on a continuing basis or when significant changes occur.

[12] *Federal Information Systems Controls Audit Manual* (GAO/AIMD-12.19.6, January 1999); *Federal Information Technology Security Assessment Framework*, November 28, 2000; GAO/AIMD-00-33, November 1999; and GAO/AIMD-98-68, May 1998.

It also does not require establishing procedures for conducting risk assessments that include the best practices outlined above. Specifically, VA's security policy requires risk to be assessed when significant changes are made to a facility or its computer systems, or at least every 3 years; however, the policy does not provide additional guidance for determining when an event is a significant change, or explaining the level of risk assessment required for system changes. In addition, VA does not have guidance on how the risk assessments should actually be conducted.

*Monitoring, Testing, and Evaluation.* Over time, policies and procedures run the risk of becoming inadequate by themselves because of changes in threats, changes in operations, or a general deterioration in the degree of agency compliance.[13] Periodic assessments or reports on threat activities can be invaluable for ensuring that adequate protections are in place and identifying needed security program improvements. Keeping summary records of actual security incidents is one way that an organization can measure the frequency of various types of violations as well as the damage suffered from these incidents. In response to our past recommendations, VA now maintains a computer security incident reporting and response process and a related information system. However, its information security management plan does not establish a mechanism for routinely analyzing security incident records. Such a practice could provide VA with an additional process for proactively identifying and responding to other system security vulnerabilities.

*Central Management Focal Point.* Our leading practices guidance also notes that managing the increased risk associated with a highly interconnected computing environment requires increased central coordination to ensure that weaknesses in one organizational unit's systems do not place the entire organization's information assets at undue risk. A central management group generally coordinates activities associated with all the elements of a comprehensive security program. This includes keeping policies and controls up to date, devising common risk assessment processes, promoting general security awareness, and monitoring an organization's security-related activities by testing controls for general support systems, accounting for the number and types of security incidents, and evaluating

[13]GAO/AIMD-00-33, November 1999.

compliance with policies. However, VA's security plan does not require independent monitoring of the near-term actions taken by facilities or responsible units to improve their security. Instead, VA relies on its administrations and staff offices to certify completion of the specific actions. Independent monitoring, however, can provide the CIO and his chief security deputy and the Secretary with assurances that actions were taken as prescribed to remedy the vulnerabilities or that the actions were consistently applied throughout the department.

VBA's On-line Application (VONAPP) Illustrates Strengths and Weaknesses of the Department's Security Program

The inherent risks involved in VA's effort to serve veterans and their families via its on-line application for compensation and pension benefits require the department to have comprehensive and rigorous security measures that protect the integrity, confidentiality, and availability of individuals' data. VBA began making this application available to veterans via the Internet in July 2000, as part of its electronic government initiative.[14] By providing this on-line capability, VA sought to offer veterans an around-the-clock alternative to submitting claims through the mail or in person. Veterans can access the application at VA's Veterans ON-line APPlication (VONAPP) Web site.

This application incorporates several security features for safeguarding the applicant's data and demonstrate implementation of VA's short-term security corrective actions aimed at improving application level access and personnel controls. These features include (1) 128-bit encryption technology to protect the data during transmission, (2) user identification and passwords to control user access to the specific application forms, (3) firewall protection to ensure that the Web and database servers that accept VONAPP applications can only be accessed by other known servers, and (4) access authorizations that are granted on a limited, need-to-know basis.

Nonetheless, this on-line VBA service continues to face potential security vulnerabilities associated with weaknesses with general support systems and operating systems access controls.

[14]Application for Compensation and Pension (VA Form 21-1900).

VA has again reported information system security general controls[15] as a material weakness in its February 2001 FMFIA report. VA needs to resolve these weaknesses affecting the overall effectiveness and security of its computer operations. Because VONAPP resides in this computer environment, it is vulnerable to inappropriate access and other security breaches affecting the department's overall computer operations. In addition, independent network assessments performed for VA by contractors last summer identified and made suggestions for correcting various vulnerabilities affecting VONAPP. However, while the contractors' work included reviews of the VONAPP Web and data base servers, it did not address vulnerabilities that have been identified in VA's wide area network, which is used to access VONAPP. Until VA addresses all of the vulnerabilities in its wide area network, it cannot ensure that applicants' data are being adequately safeguarded.

## VA Web Sites Provide Privacy Notices, But Internet Cookie Compliance Could Be Strengthened

As VA expands its offering of electronic services via the Internet and its various Web sites,[16] protecting electronic records containing personal information becomes increasingly important. Without this protection, veterans may lack the confidence to use the electronic services, and VA in turn may not be able to fully realize the benefits its Internet-based services can provide.

To ensure that individuals are informed about how their personal information is handled when they visit federal Web sites, in June 1999 OMB issued a policy memorandum requiring federal agencies to post privacy policies on their Internet Web sites.[17] The memorandum requires agencies to post easily accessible and clearly labeled privacy policies to their department or agency principal Web sites and to any other known, major entry points to their Web sites, as well

[15]General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data and programs is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

[16]A Web site is a collection of files that covers a particular theme or subject and is managed by a particular person or organization. These files are called Web pages and are usually based on hypertext markup language that may contain such elements as text, graphics, on-line audio, or video. As of February 21, 2001, VA reported having 395,587 Web pages on its Internet Web site.

[17]OMB Memorandum M-99-18, June 1999.

as any Web pages where they collect substantial personal information from the public. These policies must clearly and concisely inform visitors to the Web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it. In addition, a June 22, 2000, memorandum from OMB regarding privacy policy and data collection on federal Web sites states that federal agencies and contractors should not use persistent cookies[18] on their sites unless they provide "clear and conspicuous notice" of those activities and meet certain specified conditions.[19] Put simply, a persistent cookie is a short string of text sent from a Web server to a Web browser that is often used to recognize returning users and track Web site browsing behavior.

VA's Web sites provide a variety of information and services to its visitors. For example, table 1 provides information on VA Web sites where individuals can electronically access and complete ten specific application forms on-line. In accordance with OMB's Web privacy requirements, VA has developed a privacy and security statement for its primary Web site, www.va.gov. In addition, VA requires its administrations and staff offices to link their individual Web sites to the primary site or to post privacy policies on their individual sites that are consistent with OMB's guidance. The privacy and security statements posted on VA's primary and related Web sites are consistent with OMB's requirements for being clear, concise, clearly labeled, and easily accessed.

[18]Persistent cookies specify expiration dates, remain stored on the client's computer until the expiration date, and can be used to track users' browsing behaviors by identifying their Internet addresses whenever they return to a site.
[19]These conditions are (1) a compelling need to gather the data on the site, (2) appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (3) personal approval of the agency head.

Table 1. VA Application Forms on the Internet.[a]

| VA Admin-istration[b] | VA form number | Application form | Description | VA Web address |
|---|---|---|---|---|
| VHA | 10-10EZ | Application for Health Benefits | Application to enroll for health benefits | http://www.1010ez.med.va.gov/sec/vha/1010ez/ |
| VHA | 10-2850 | Application for Physicians, Dentists, Podiatrists, and Optometrists | Application for employment | http://www.vacareers.com/pages/3.b.3.x.htm |
| VHA | 10-2850a | Application for Nurses and Nurse Anesthetists | Application for employment | Http://www.vacareers.com |
| VHA | 10-2850c | Application for Associated Health Occupations | Application for employment for occupational therapists, pharmacists, etc. | http://www.vacareers.com |
| VBA | 21-1900 | Veterans Online APPlication (VONAPP) | Applications for compensation and pension benefits and for vocational rehabilitation benefits | http://www.vabenefits.vba.va.gov |
| VBA | 22-1999<br>22-1999b | VA Online Certification (VAnetCert) | Application for school officials to certify eligibility for educational benefits | http://www.gibill.va.gov |
| VBA | 22-8979 | Web Automated Verification of Enrollment (WAVE) | Application for education enrollment reporting | http://www.gibill.va.gov |
| VBA | 26-1805 | Request for Determination of Reasonable Value (via VA Assignment System) | Application requesting a determination of reasonable value for realty used as security for VA mortgages | http://vaas.vba.va.gov/prod/vaas/indexnew.cfm |

[a] Two of the on-line applications—VAnetCert and WAVE—are not currently accessible via the Internet and thus were not available for our evaluation.
[b] NCA does not provide on-line applications for public use.

In addition, we confirmed that other VA Web sites providing forms that may be downloaded[20] also contain links to the privacy and security statement posted on VA's primary Web site. And as further evidence of the department's attention to privacy policies, VA Web sites containing the applications for health benefits and for compensation and pension and vocational rehabilitation require users to acknowledge that they have read additional privacy notices prior to providing personal information.

While VA has adhered to Web privacy requirements, it has not consistently adhered to OMB's requirement limiting the use of persistent cookies. In interviews with VA Privacy Act officials and Webmasters, we were told that the department was in compliance with the OMB policy and did not use persistent cookies on its Internet Web sites. However, during the course of our work, we identified and informed VA of persistent cookies on two Web pages used to access VBA on-line applications. In discussing this finding, VA's Privacy Act officer said that VBA did not have departmental approval to use these cookies, and stated that the department would look into the matter.

## IMPROVEMENTS MADE IN VA's IT INVESTMENT MANAGEMENT, BUT CHALLENGES REMAIN

IT investment management processes provide a systematic method for agencies to minimize risks while maximizing their return on IT investments. Our September 2000 testimony[21] pointed out that while VA had improved its processes for selecting, monitoring, and managing Capital Investment Board (CIB)-level projects, a more structured decision process was needed for IT projects below the CIB threshold. Moreover, we noted that VA needed to conduct more timely in-process reviews and provide lessons learned from post-implementation reviews to key decisionmakers, such as investment panel members. In-process reviews are essential because they enable management to make informed, data-driven decisions about the progress of IT

[20]VA administrations' Web sites contain 114 public-use forms that individuals can download and submit to the department through means other than these Web sites.
[21] GAO/T-AIMD-00-321, September 21, 2000.

projects at key milestones in their life cycles, including whether to cancel, modify, or continue the projects. In addition, post-implementation reviews at the conclusion of key project phases provide critical information that management can use to validate projected savings and identify needed changes in systems development and IT management practices.

Subsequent to our September testimony, VA provided us its *Information Technology Capital Investment Guide.* Intended as departmentwide guidance for use in each of VA's components, it provides comprehensive guidelines for processes to be used in managing the department's IT investments. The guide addresses a number of shortcomings we previously identified with VA's investment management process and reflects the attention that the department has devoted to improving the process.

Let me mention a few of these positive changes. Specifically, for projects below the CIB dollar threshold, VA now requires its administrations and offices to evaluate and report on the progress of its IT projects at predetermined intervals. For example, organizations are to submit to the director of VA's Information Resources Management Planning and Acquisitions Service quarterly project status reports summarizing accomplishments, problems encountered, and corrective actions taken. In addition to these reports, organizations are to notify the director of any significant changes to the overall project, plan, schedule, or benefit-cost information at the time those changes are made. The guide also requires administrations and staff offices to manage smaller IT projects, and to track IT expenditures and other data. Further, consistent with our prior recommendations, VA has stipulated in the guide that completion dates be included in in-process review plans and that the results of post-implementation reviews of CIB-level projects be provided to VA's CIO Council.

Nevertheless, VA has not yet demonstrated that it is implementing key parts of its investment guidance. For example, since September 2000, it has not scheduled or conducted any in-process or post-implementation reviews. VA has indicated that it intends to conduct one in-process review (of its E-Commerce system) and three post-implementation reviews. However, at the

conclusion of our work last month, VA had not established plans or schedules indicating when they would be conducted. In addition, although the guidance requires VA to conduct quarterly execution reviews of approved IT capital investments to help identify projects experiencing cost, schedule, or performance problems (and thus candidates for in-process reviews), the Director of VA's IRM Planning and Acquisition Service stated that VA has not conducted an IT execution review since June 2000.

We also testified last September[22] that VA had not implemented a uniform mechanism for collecting, automating, and processing data on IT costs and performance across the department. At that time, VBA tracked IT expenditures centrally, while VHA delegated responsibility for tracking approximately 80 percent of its IT expenditures to the 22 VISNs. Further, neither of these administrations tracked personnel costs associated with their IT projects because of the limitations of VA's financial management system.

A uniform cost-tracking mechanism should provide data needed to monitor and evaluate investments individually and strategically, provide feedback on the project's adherence to strategic initiatives and plans, and allow for review of unexpected costs or benefits that resulted from investment decisions.[23] An expenditure tracking mechanism would also aid the department in meeting the requirements of its own Directive 6000, which requires officials to maintain complete and accurate data on all personnel and nonpersonnel costs associated with IT activities.

According to the director of IRM Planning and Acquisition Service, VA will begin using a numbering system within the financial management system to track IT capital investment costs beginning with the execution of fiscal year 2002 projects. Using this numbering system, the Information Resources Management Planning and Acquisitions Service will run special reports on project expenditures on an as-needed basis. However, the system will not allow VA to track personnel costs for IT projects automatically. VA plans to extend the numbering scheme to other

[22]GAO/AIMD-00-321, September 21, 2000.
[23]GAO/AIMD-10.1.23.

projects once its new financial management system is implemented in October 2004. In the interim, the VA CIO Council is investigating the use of a universal project management tool with personnel tracking capability.

## VA REMAINS WITHOUT AN ENTERPRISEWIDE ARCHITECTURE

The Clinger-Cohen Act and Office of Management and Budget guidelines direct agency CIOs to implement an architecture to provide a framework for evolving or maintaining existing IT and for acquiring new IT to achieve the agency's strategic goals. Leading organizations both in the private sector and in government use enterprise architectures to guide mission-critical systems development and to ensure the appropriate integration of information systems through common standards.[24] Further, in recently issued guidance,[25] the CIO Council has emphasized the importance of enterprise architectures for evolving information systems and developing new systems that optimize an organization's mission value.

In previous testimony, we noted that VA had adopted the National Institute of Standards and Technology (NIST) five-layer model[26] as the framework that it planned to use for its departmentwide IT architecture. VA also published a departmentwide technical architecture,[27] which described one layer—the technology layer—of the NIST model. In response to a May 11, 2000,[28] hearing, the former Chairman of this Subcommittee requested that VA provide a plan and milestones for completing the logical portion of its departmentwide architecture within 60 days of that hearing. VA subsequently submitted a two-page plan to the Subcommittee that provided a high-level discussion of VA's approach to developing a departmentwide logical architecture and time estimates for various deliverables. The approach outlined in the plan called for each VA administration to develop its own logical architecture, but to avoid duplicating the

---

[24] *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology—Learning from Leading Organizations* (GAO/AIMD-94-115, May 1994).
[25] *A Practical Guide to Federal Enterprise Architecture*, February 2001, Federal Architecture Working Group and Federal Chief Information Officers Council.
[26] The five layers are business processes, information flows and relationships, applications processing, data descriptions, and technology. This provides a framework for defining an IT architecture.
[27] *VA Technical Architecture: Technical Reference Model and Standards Profile,* May 1999.
[28] GAO/T-AIMD-00-74, May 11, 2000.

administrations' efforts, VA planned to develop a departmentwide component that focused on crosscutting issues and interdependencies. However, as we noted in our September 2000 testimony,[29] this approach would not likely result in an integrated architecture but, rather, in at least three different architectures. Accordingly, we pointed out the need for VA to reassess its strategy and work together with the administrations to develop an integrated, departmentwide logical architecture, consistent with the Clinger-Cohen Act.

Developing an enterprise architecture requires a disciplined and rigorous approach that is endorsed by senior management. The CIO Council's enterprise architecture guide stresses that an enterprise architecture is a corporate asset that should be managed as a formal, long-term program, and that successful execution of the enterprise architecture process is an agencywide endeavor requiring management, allocation of resources, continuity, and coordination. In particular, the architecture development team needs to work closely with agency business line executives to produce a description of the agency's operations, a vision of the future, and an investment and technology strategy for accomplishing defined business goals.

After being confronted with contractor bids for developing the logical architecture for the department that exceeded available resources in October 2000, VA's acting CIO and the administration CIOs agreed to undertake an accelerated in-house effort to develop a draft departmentwide IT architecture by March 2, 2001. This effort was to combine the IT architectural work that had been completed by VA's administrations and offices into one draft IT architecture plan for the department.

As of the end of March 2001, VA had not yet completed the integrated, departmentwide architecture. According to the architecture project manager, the Secretary recently redirected efforts toward developing this architecture and requested that the architecture team prepare a plan detailing a new strategy for developing it. The Secretary was concerned, in part, that VA's business lines had not been adequately integrated in the prior effort to develop the architecture, and has requested that VA business managers be included in the new development effort.

[29]GAO/T-AIMD-00-321, September 21, 2000.

## TWO SYSTEMS PROJECTS ARE PROGRESSING, BUT FACE CRITICAL CHALLENGES UNDERLYING SUCCESSFUL UTILIZATION

You also asked that we update you on VA's progress with two visible systems projects, VHA's Decision Support System (DSS) and VBA's compensation and pension replacement (C&P) project, one of the major initiatives under the agency's Veterans Service Network (VETSNET) strategy.

DSS is an executive information system designed to provide VHA managers and clinicians with data on patterns of patient care and patient health outcomes, as well as the capability to analyze resource utilization and the cost of providing health care services. In September 2000,[30] we testified that DSS had not been fully utilized since its implementation at all VA medical centers in October 1998. We noted that while cost reductions and improved clinical processes had been reported by some VISNs and medical centers using DSS, none of the ones we had contacted used DSS for all of the purposes VHA intended. At that time, the reasons given by VISNs and medical centers for not making greater use of DSS included (1) concerns about the accuracy and completeness of DSS data and (2) DSS staffing issues, including insufficient staff, staff with inadequate skills, and staff turnover.

Since last September, VHA has made moderate progress in increasing usage of DSS among its VISNs and medical centers. At the time of that testimony, 4 of 22 VISNs—VISN 6 (Durham, North Carolina), VISN 8 (Bay Pines, Florida), VISN 20 (Portland, Oregon), and VISN 21 (San Francisco)—had not provided examples of how they were using DSS. However, in recent discussions with the DSS coordinators at these VISNs, three of the four provided examples of their current use of DSS information or of initiatives underway to facilitate greater use.

For example, to facilitate clinical decisionmaking, these DSS coordinators told us they are using DSS to provide VISN-wide information on:

[30] GAO/T-AIMD-00-321, September 21, 2000.

the pharmacy cost of hepatitis C, radiology utilization for preoperative chest x-rays among eye surgery patients, and the frequency with which pathology laboratory medical tests are administered;

patient length of stay and cost per case, to help determine the extent to which medical centers are meeting an established performance measure of reducing the cost of chronic obstructive pulmonary disease by 5 percent; and

a VISN-wide diabetes study to determine what percentage of patients with a primary or secondary diagnosis of diabetes had received certain required testing within a specified time frame.

However, VISN 20 (Portland) reports that it is still not using DSS. According to the DSS coordinator, because of differences in the structural organization of DSS among the VISN's facilities, DSS data maintained by the VISN's medical centers cannot be compared, and thus not readily useable for decisionmaking. For example, she explained that in maintaining primary care data in DSS, a community-based outpatient clinic may include data in its DSS primary care department that extends beyond just primary care work, while the medical facilities only include primary care work in their DSS primary care departments.

Our September testimony[31] also reported on the medical centers' use of DSS. At that time, 59 of 140 centers had not provided specific examples of DSS use.[32] Three of the 59 medical centers—Beckley (West Virginia), Anchorage Health Care System, and Boise (Idaho)—had explicitly stated that they did not use DSS. However, in contrast, two of the medical centers—Long Beach and Portland (Oregon)—reported extensive use of DSS. We met with physicians, nurses, and administrators at these two medical centers to better understand the reasons behind higher DSS usage at these centers. They pointed to numerous positive examples where DSS was useful:

Changing the clinical practice of admitting elective surgery patients the day of surgery,

Determining whether physicians are following accepted clinical guidelines for treating atrial fibrillation patients,

[31] GAO/T-AIMD-00-321, September 21, 2000.

[32] These 59 medical centers did not provide specific examples of DSS use in their response to the March 2000 memo. This does not necessarily mean that they were not using DSS. For example, none of the medical centers in VISN 13 provided examples; however, DSS data is used more extensively at the VISN level in that VISN than in any other.

Determining the location of community-based outpatient clinics to provide service to the most veterans,

Assessing the quality of care given to a certain cohort of patients,

Evaluating the effectiveness of a case management model of nursing care delivery, and

Determining staffing levels and the required mix of nurses for wards.

Factors Contributing to Successful Use of DSS

In on-site discussions with officials at the Long Beach and Portland medical centers, they pointed out several factors that had substantially contributed to the successful use of DSS:

*Top management support*—Each center's director had set an explicit expectation that decisions would be made based on DSS data and that concerns about data quality would not be an acceptable excuse for not using the system.

*Skilled DSS staff*—At each center, the director had assigned staff with adequate skills to use DSS, thus providing the necessary resources to ensure that it functioned properly and that proper assistance was available to administrators and medical staff in analyzing and using DSS data. Further, the DSS staff was knowledgeable in both the financial and clinical aspects of the centers' work, which substantially facilitated use of the system.

*Familiarity with DSS and longevity of experience*—DSS had been implemented at the medical centers during the first phase of its implementation, and DSS site managers at both medical centers had been with DSS since its inception.

Efforts encouraging greater VA-wide use of DSS are continuing. Fiscal year 2000 DSS data are being used as part of the fiscal year 2002 resource allocation process; use and validation of DSS data are among the factors that will be considered in determining VISN director year-end performance appraisals; and VISN directors have been required to provide monthly examples of their reports and/or processes that rely on DSS data, and to ensure that the processing of DSS data by their medical centers is current (i.e., no more than 60 days old).

The new DSS program office—established March 11, 2001—is also developing project plans for priority initiatives, which are to be integrated into a business plan by the end of May. Later, through review of best practices and benchmarking, the program office plans to develop opportunities to export and apply measures derived from DSS data. In doing this, it remains critical that VHA continue to provide top management support to ensure that the system is fully utilized and benefits are being realized in both the financial and clinical areas.

## THE COMPENSATION AND PENSION PAYMENT SYSTEM REPLACEMENT CONTINUES TO FACE CHALLENGES

The C&P project was intended to replace VBA's existing compensation and pension payment systems with one new, state-of-the-art system. The project, which began in April 1996, had an estimated cost of $8 million and was originally scheduled for completion in May 1998.

Over the years, we and VA have reported on the problems that VBA has encountered in completing this project.[33] Our prior work found that the project had been delayed largely because VBA lacked an integrated architecture defining its business processes, information flows and relationships, business requirements, and data descriptions. Specifically, the project was begun before VBA had fully developed its business requirements and delays subsequently resulted from confusion over the specific requirements to be addressed. In addition, our prior work also attributed the project's problems to VBA's immature software development capability.[34]

Last September, we testified[35] that VBA had changed its strategy for developing this new system to one that utilized and built upon software products developed elsewhere in VBA. At that time, however, VBA did not have an integrated project plan and schedule detailing all of the areas that

---

[33] *Veterans Benefits Modernization: Management and Technical Weaknesses Must Be Overcome if Modernization Is To Succeed* (GAO/T-AIMD-96-103, June 19, 1996), *Veterans Benefits Computer Systems: Risks of VBA's Year 2000 Program* (GAO/AIMD-97-79, May 30, 1997), and *VETSNET Quarterly Review*, Office of Information Resources Management, Department of Veterans Affairs, March 1998.
[34] *Veterans Benefits Modernization: VBA Has Begun to Address Software Development Weaknesses But Work Remains* (GAO/AIMD-97-154, September 15, 1997).
[35] GAO/T-AIMD-00-321, September 21, 2000.

needed to be addressed in order to develop and implement the system but, rather, only short-term schedules for developing five key software components.

The C&P project has moved forward since last September. In November 2000, VBA completed implementation of a rating board automation tool and completed development and testing of the other four software products at the end of January 2001—about 1 month behind schedule. A small pilot test was conducted in mid-February to demonstrate VBA's ability to process and generate compensation and pension benefit payments and according to VBA, the test occurred without problems and successfully demonstrated that claims payments could be made using the new products. VBA has also taken steps to improve its planning and management of this effort. For example, VBA has created a project control board to provide day-to-day management and oversight for the project, and it has begun allocating staff to conduct work supporting key areas that had not been addressed previously, including data conversion, interfaces, batch processing, and synchronization. In addition, VBA has released a schedule that calls for deploying the compensation and pension replacement system in July 2002.

Nonetheless, VBA still needs to address several important issues before it can successfully implement the project. For example, although it has established a schedule for deploying the project, it has not developed an integrated project plan and schedule incorporating all of the critical areas of this system development effort, to be used as a means of determining what needs to be done and when, and of measuring progress. Instead, detailed plans and schedules exist only for portions of it, while other areas have yet to be fully addressed, including critical areas such as data conversion. As we reported in September, data conversion is considered by VBA to be the most difficult remaining part of the compensation and pension replacement project.

Furthermore, VBA's C&P pilot test only processed ten original claims that did not require significant claims development work. The current C&P payment system processes on the order of 3.2 million payments each month. Therefore, VBA must address scalability issues in order to move this software from the pilot stage to the deployment stage. The limited scope and nature of the pilot test puts VBA's millions of claims at risk should the C&P application not work as intended once it is put into an organizationwide operational setting.

- - - - -

In summary, Mr. Chairman, while VA has taken actions to improve many of its IT management processes, it continues to face substantive challenges which if left incomplete can disrupt existing progress and threaten the viability of its existing and future IT spending. VA has yet to fill its full-time department CIO vacancy since the position's creation 3 years ago. In addition, sustained leadership and commitment are necessary for improving VA's departmentwide computer security program, particularly effectively addressing and monitoring security risks as it takes steps to move some of its information and services to veterans onto the Internet. And while the department has done a good job of posting privacy and security notices on its Web sites, it should nevertheless increase its attention to compliance with OMB policies prohibiting the use of persistent Internet cookies. Further, until VA defines and begins to implement a departmentwide, enterprise architecture, it will continue to encounter costly difficulties in achieving its "One VA" vision. Finally, VA faces important decisions for making greater use of DSS and in ensuring that it is making an informed decision regarding continued development and wide-scale implementation of the compensation and pension replacement project. Continued attention and full implementation of past recommendations we and others have made are essential for achieving better IT management outcomes.

## SCOPE AND METHODOLOGY

We performed this assignment in accordance with generally accepted government auditing standards, from December 2000 through April 2001. In carrying out this assignment we assessed the structure of and VA's efforts to fill its CIO position; improve the department's computer security; processes for selecting, controlling, and evaluating IT investments; complete a departmentwide integrated systems architecture; track its IT expenditures; utilize VHA's Decision Support System; and implement VBA's compensation and pension replacement project.

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

## CONTACTS AND ACKNOWLEDGMENTS

For information about this testimony, please contact me at (202) 512-6257 or by e-mail at mcclured@gao.gov. Individuals making key contributions to this testimony include Mary J. Dorsey, Amanda C. Gill, Tonia L. Johnson, David W. Irvin, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, and Charles M. Vrabel.

(310406)

**Orders by Internet**

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to

info@www.gao.gov

or visit GAO's World Wide Web home page at

http://www.gao.gov

**To Report Fraud, Waste, and Abuse in Federal Programs**

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: 1-800-424-5454