United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10 a.m. EDT
Thursday,
September 26, 2002

VA INFORMATION TECHNOLOGY

Management Making Important Progress in Addressing Key Challenges

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

GAO-02-1054T

GAO
Accountability★Integrity★Reliability

Highlights

VA INFORMATION TECHNOLOGY Management Making Important Progress in Addressing Key Challenges

Highlights of GAO-02-1054T, testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In March of this year, GAO testified before the Subcommittee about the Department of Veterans Affairs' (VA) information technology (IT) program, and the strides that the Secretary had made in improving departmental leadership and management of this critical area–including the hiring of a chief information officer.

At the Subcommittee's request, GAO evaluated VA's new IT organizational structure, and provided an update on VA's progress in addressing other specific areas of IT concern and our related recommendations pertaining to

- enterprise architecture,
- information security,
- the Veterans Benefits Administration's replacement compensation and pension payment system and maintenance of the Benefits Delivery Network, and
- the government computer-based patient record initiative.

What GAO Found

Since our March testimony, VA has made important progress in its overall management of information technology. For example, the Secretary's decision to centralize IT functions, programs, and funding under the department-level CIO holds great promise for improving the accountability and management of IT spending–currently over $1 billion per year. But in this as well as the other areas of prior weakness, the strength of VA's leadership and continued management commitment to achieving improvements will ultimately determine the department's degree of success. As for its progress in other areas:

- *Enterprise architecture.* The Secretary recently approved the initial, "as is" version of this blueprint for evolving its information systems, focused on defining the department's current environment for selected business functions. VA still, however, needs to select a permanent chief architect and establish a program office to facilitate, manage, and advance this effort.
- *Information security.* Steps have been taken that should help provide a more solid foundation for detecting, reporting, and responding to security incidents. Nonetheless, the department has not yet fully implemented a comprehensive computer security management program that includes a process for routinely monitoring and evaluating the effectiveness of security policies and controls, and acting to address identified vulnerabilities.
- *Compensation and pension payment system.* While some actions have been taken, after more than 6 years, full implementation of this system is not envisioned before 2005; this means that the 3.5 million payments that VA makes each month will continue to depend on its present, aging system.
- *Government computer-based patient record initiative.* VA and the Department of Defense have reported some progress in achieving the capability to share patient health care data under this program. Since March, the agencies have formally renamed the initiative the Federal Health Information Exchange and have begun implementing a more narrowly defined strategy involving a one-way information transfer from Defense to VA; a two-way exchange is planned by 2005.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to take part in your discussion of the Department of Veterans Affairs' (VA) information technology (IT) program. Information technology continues to play an integral and substantial role in helping VA effectively serve our nation's veterans, with the department spending more than a billion dollars annually in support of its information technology operations. As you are well aware, however, the department has been challenged in its efforts to effectively manage its information technology to produce results and achieve optimal agency performance.

Our testimony last March noted important strides by the Secretary of Veterans Affairs to improve the department's IT leadership and management, including the hiring of a chief information officer (CIO) to lead the program and a commitment to reform how the department uses information technology.[1] Since that time, the Secretary has taken additional steps toward achieving improvements in key areas of IT performance, including recently announcing a realignment of the way in which the department is organized to carry out its information technology mission.

At your request, we will discuss today this new organizational structure and resulting changes in the role of VA's CIO. In addition we will provide an update of the department's progress since March in addressing specific weaknesses in its overall information technology program, including the status of its actions to

- develop an enterprise architecture,
- improve information security,
- implement the Veterans Benefits Administration's (VBA) veterans service network (VETSNET) replacement compensation and pension payment system and maintain the existing Benefits Delivery Network, and
- implement jointly with the Department of Defense and Indian Health Service the government computer-based patient record initiative.

In conducting this work we analyzed relevant documentation and interviewed key agency officials to identify and assess VA's decisions and

[1]U.S. General Accounting Office, *VA Information Technology: Progress Made, but Continued Management Attention Is Key to Achieving Results*, GAO-02-369T (Washington, D.C.: Mar. 13, 2002).

actions since March to improve its information technology management. We reviewed available documentation discussing the department's plans and strategies for realigning its information technology structure. We also examined its enterprise architecture strategy as well as steps being taken to strengthen computer security management departmentwide. Further, we conducted site visits at the Veterans Benefits Administration's regional office in Salt Lake City to assess the current use of VETSNET in processing compensation and pension benefits claims; and at the VA medical center in Washington, D.C., to observe data retrieval capabilities of the Federal Health Information Exchange (formerly the government computer-based patient record initiative). We performed our work in accordance with generally accepted government auditing standards, in August and September of this year.

Results in Brief

Over the past 6 months, VA has shown clear progress in addressing some of the critical weaknesses that have plagued its management of information technology. The Secretary of Veterans Affairs and other top agency leaders have continued to make important strides in improving key areas of IT performance. Nonetheless, some aspects of the department's information technology environment continue to be particularly challenging and to require substantial management attention. As the department proceeds, ensuring sound project management and oversight will continue to be essential to advancing its efforts.

Accountability for its information technology investments should be well served by VA's recently announced realignment of its information technology structure. Although yet to be finalized, the Secretary's decision to centralize information technology functions, programs, and funding under the department-level CIO shows promise for improving IT accountability and enabling the department to implement its One VA vision.[2] The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively capture and manage its IT spending.

[2]According to the department, the "One VA" vision describes how it will use information technology in versatile new ways to improve services and enable VA employees to help customers more quickly and effectively. It stems from the recognition that veterans think of VA as a single entity, but often encounter a confusing, bureaucratic maze of uncoordinated programs that put them through repetitive and frustrating administrative procedures and delays.

Beyond its actions to establish greater accountability in this area, the department continues to make important progress in developing its departmentwide enterprise architecture—the blueprint for evolving its information systems and developing new systems that optimize their mission value. The Secretary recently approved the initial version of VA's enterprise architecture, focused on defining the department's current, "as is" and desired, "to be" target environments for selected business functions. Nonetheless, VA must still accomplish critical actions to ensure successful completion of its architecture. For example, to achieve a sound program management structure, it needs to select a permanent chief architect and establish a program office to facilitate, manage, and advance this effort.

In another critical area, the department continues to make progress in strengthening its information security. It has taken actions that should help provide a more solid foundation for detecting, reporting, and responding to security incidents. Among these actions, it has contracted to expand departmentwide incident response and analysis capabilities, including enhancing security monitoring and detection. Nonetheless, the department has not yet fully implemented a comprehensive computer security management program that includes a process for routinely monitoring and evaluating the effectiveness of security policies and controls and addressing identified vulnerabilities. Further, VA's offices self-report computer security weaknesses, and it lacks an independent component to ensure the accuracy of reporting and validation of corrective actions taken.

Conversely, the department is not making as much progress in addressing the challenges associated with implementing its VETSNET compensation and pension replacement payment system. Specifically, after more than 6 years, the department still has significant work to accomplish, and could be several years from fully implementing the system. Complete implementation is not anticipated until 2005, thus requiring continued reliance on the aging Benefits Delivery Network to provide the more than 3.5 million payments that VA must make to veterans each month.

Finally, VA and DOD have made some progress in achieving the capability to share patient health care data begun under the government computer-based patient record (GCPR) initiative. This progress was achieved as part of a substantially revised, scaled-down strategy. As part of this new strategy that the two agencies have now implemented, clinicians in VA medical facilities throughout the country have access to health information on more than a million separated service personnel.

IT Realignment Increases Authority and Oversight of VA's Chief Information Officer

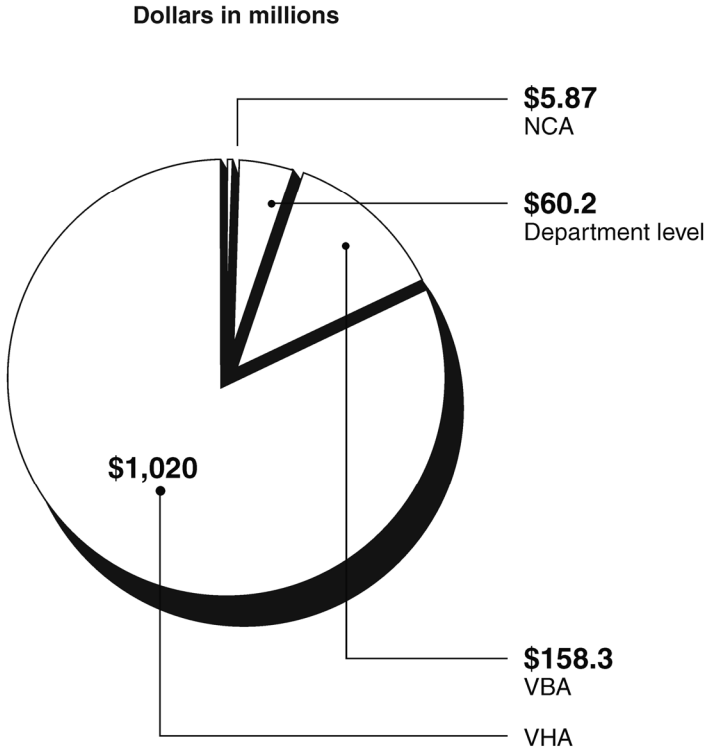
Successful implementation of VA's information technology program requires strong leadership and management to help define and guide the department's plans and actions. The Paperwork Reduction Act of 1980 and the Clinger-Cohen Act of 1996[3] articulate the importance of CIOs in promoting improvements in their agencies' work processes and making sound investment decisions that effectively align IT projects with the organization's business planning and measurement processes. To be successful in this role, CIOs must build credible organizations and develop and organize information management capabilities to meet agency mission needs.

With the hiring of a department-level CIO in August 2001, VA took a significant step toward addressing critical and longstanding weaknesses in its management of information technology. Our prior work has highlighted some of the challenges that the CIO faced as a result of the way in which the department was organized to carry out its information technology mission.[4] Among these challenges was that information systems and services were highly decentralized, with the VA administrations and staff offices controlling a majority of the department's information technology budget. As illustrated in figure 1, out of the approximately $1.25 billion fiscal year 2002 information technology budget, the Veterans Health Administration (VHA) oversaw approximately $1.02 billion, VBA approximately $158.3 million, and the National Cemetery Administration (NCA) approximately $5.87 million. The remaining $60.2 million was controlled at the department level.

[3]44 U.S.C. 3506 and P.L. 104-106, Section 5125, respectively.

[4]U.S. General Accounting Office, *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist*, GAO-01-550T (Washington, D.C.: Apr. 4, 2001) and GAO-02-369T.

Figure 1: Breakdown of VA's $1.25 Billion Information Technology Budget (fiscal year 2002)



Source: GAO analysis.

In addition, our testimony in March noted that there was neither direct nor indirect reporting to VA's cyber security officer—the department's senior security official—thus raising questions about this person's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. The more than 600 information security officers in VA's three administrations and its many medical facilities throughout the country were responsible for ensuring the department's information security, although they reported only to their facility's director or to the chief information officer of their administration.

Given the large annual funding base and decentralized management structure, it is crucial that the CIO ensure that well-established and integrated processes for leading, managing, and controlling investments

are commonplace and followed throughout the department. The Secretary has recognized weaknesses in accountability for the department's information technology resources and the consequent need to reorganize how information technology is managed and financed. Accordingly, in a memorandum dated August 6, 2002, he announced a realignment of the department's information technology operations. According to the memorandum, the realignment will centralize information technology functions, programs, workforce personnel, and funding into the office of the department-level CIO. In particular, several significant changes are being made:

- The CIOs in each of the three administrations—VHA, VBA, and NCA—have been designated deputy CIOs and will report directly to the department-level CIO. Previously, these officials served as component-level CIOs who reported only to their respective administrations' undersecretaries.
- All administration-level cyber security functions have been consolidated under the department's cyber security office, and all monies earmarked for these functions have been placed under the authority of the cyber security officer. Information security officers previously assigned to VHA's 21veterans integrated service networks will now report directly to the cyber security officer, thus extending the responsibilities of the cyber security office to the field.
- Beginning in fiscal year 2003, the department-level CIO will assume executive authority over VA's IT appropriations.

The realignment had not been finalized at the conclusion of our review, thus its full impact on VA's mission and the CIO's success in managing information technology at the department level could not yet be measured. Nonetheless, in pursuing these reforms, the Secretary has demonstrated the significance of establishing an effective management structure for building credibility in the way information technology is used, and has taken a significant step toward achieving a "One VA" vision.

The Secretary's initiative also represents a bold and innovative step by the department, and is one that has been undertaken by few other federal agencies. For example, as part of our review, we sent surveys to the 23 other major federal agencies, seeking information on the organization and reporting relationships of their department- and component-level CIOs. Of the 17 agencies that responded, 8 reported having component-level CIOs, none of which reported to the department-level CIO. Only one agency with component-level CIOs reported that its department-level CIO had authority over all IT funding.

As the realignment proceeds, the CIO's success in managing information technology operations will hinge on effective collaboration with business counterparts to guide IT solutions that meet mission needs. Guidance that we issued in February 2001 on the effective use of CIOs in several leading private and public organizations provides insight into three key factors contributing to CIO successes:

- First, senior executives embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making.
- 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 earn credibility and produce results by establishing effective working relationships with business unit heads.
- Third, successful CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy 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.[5]

VA's new organizational structure holds promise for building a more solid foundation for investing in and improving the department's accountability over information technology resources. Specifically, under the realignment the CIO assumes budget authority over all IT appropriations, including authority to veto proposals submitted from sub-department levels. This could have a significant effect on VA's accountability for how components are spending money, as we have previously noted the department's inability to adequately capture all of its IT costs.[6]

As the first step toward gaining accountability for information technology investments, the CIO is attempting to determine what expenditures have been incurred in fiscal year 2002. Since VA's annual budget submissions to OMB have not included a specific line item for information technology operations, the CIO has asked each administration to provide accurate information identifying the costs incurred by each of them for this fiscal

[5]U.S. General Accounting Office, *Maximizing the Success of Chief Information Officers: Learning From Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

[6]U.S. General Accounting Office, *VA Information Technology: Progress Continues Although Vulnerabilities Remain*, GAO/T-AIMD-00-321 (Washington, D.C.: Sept. 21, 2000).

year. According to the CIO, preliminary results showed that certain non-IT costs, such as for users' personnel, had been included in the total expenditures, while some IT costs, such as for IT personnel and telecommunications, had been excluded. The CIO's goal is to compile cost data that accurately reflect the department's information technology expenditures.

In the absence of a budget line item, the CIO is requiring each facility to develop "spend plans" for fiscal year 2003 IT funding. These plans are expected to serve as a control mechanism for information technology expenditures during the year and will be administered by each facility, with the CIO retaining veto power over them. The plans have been designed to provide the CIO with investment cost details at a departmentwide level, allowing for a portfolio-based project selection process and lessening duplication of effort. Once the plans are implemented, the CIO anticipates being able to compare planned and actual expenditures and to uncover the details of specific projects.

Progress Toward Developing an Enterprise Architecture Continues, but Additional Work Needed

Developing and implementing an enterprise architecture[7] to guide VA's information technology activities continues to be an essential and challenging undertaking. VA and other federal agencies are required to develop and implement enterprise architectures to provide a framework for evolving or maintaining existing and planned IT, in accordance with OMB guidelines.[8] In addition, guidance issued last year by the Federal CIO Council,[9] in collaboration with us, further emphasizes the importance of enterprise architectures in evolving information systems, developing new systems, and inserting new technologies that optimize an organization's mission value. Overall, effective implementation of an enterprise architecture can facilitate VA's management by serving to inform, guide, and constrain the information technology investment decisions being made for the department, and subsequently decreasing the risk of buying

[7]An enterprise architecture is a blueprint for systematically and completely defining an organization's current (baseline) operational and technology environment, and a roadmap toward the desired (target) state. It is an essential tool for effectively and efficiently engineering business processes and for implementing their supporting systems and helping them evolve.

[8]OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: Nov. 30, 2000).

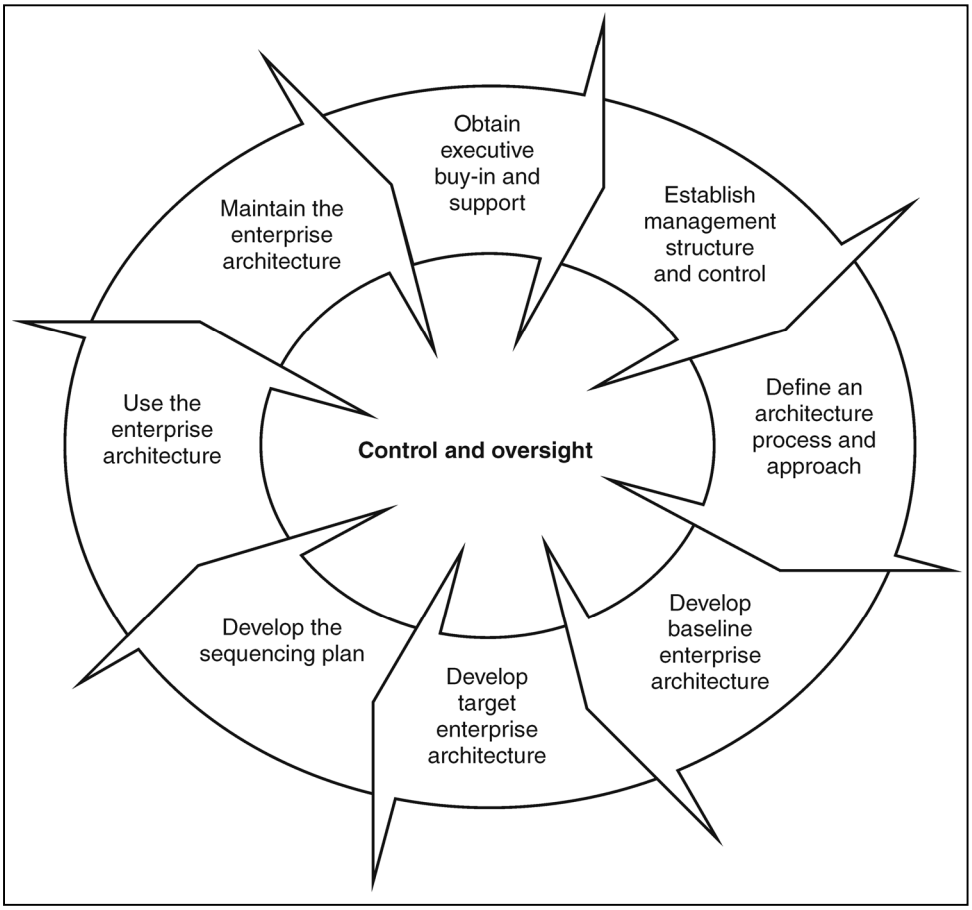
[9]Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (Washington, D. C.: February 2001).

and building systems that are duplicative, incompatible, and unnecessarily costly to maintain and interface.

As depicted in figure 2, the enterprise architecture is both dynamic and iterative, changing the enterprise over time by incorporating new business processes, new technology, and new capabilities. Depending on the size of the agency's operations and the complexity of its environment, enterprise architecture development and implementation require sustained attention to process management and agency action over an extended period of time. Once implemented, the enterprise architecture must be kept current through regular maintenance.

Periodic reassessments are required to ensure that it remains aligned with the department's strategic mission and priorities, changing business practices, funding profiles, and technology innovation.

Figure 2: The Enterprise Architecture Process



Source: A Practical Guide to Federal Enterprise Architecture, Version 1.0, 2001

When we testified last March, VA had taken a number of promising steps toward establishing some of the core elements of an enterprise architecture. Among other actions, it had obtained executive commitment from the Secretary, department-level CIO, and other senior executives and business teams that is crucial to raising awareness of and leveraging participation in developing the architecture. VA had also chosen a highly recognized framework to organize the structure of its enterprise

architecture.[10] Further, it had begun defining its current architecture, an important step for ensuring that future progress can be measured against such a baseline, and it was developing its future (target) telecommunications architecture.

Nonetheless, at that time we noted that VA still faced many more critical tasks to successfully develop, implement, and manage its enterprise architecture. One of the key activities that required attention was the establishment of a program management office headed by a permanent chief architect to manage the development and maintenance of the enterprise architecture. In addition, the department needed to complete a program management plan delineating how it would develop, use, and maintain the architecture. Further, although VA had developed a baseline application inventory to describe its "as is" state, it had not completed validating the inventory or developing detailed application profiles for the inventory, including essential information such as business functions, information flows, and external interface descriptions.

VA Has Expanded Its Initial Enterprise Architecture Development Work

Over the past 6 months, VA has made substantial strides toward instituting its enterprise architecture program. For example, in April it issued its fiscal year 2002 One VA enterprise architecture implementation plan, which will be used to align integrated technology solutions with the department's business needs. And in July, the CIO issued a mandatory directive prescribing departmentwide policy for the establishment and implementation of an integrated One VA enterprise architecture and to guide the development and management of all of VA's IT assets.[11] VA also finalized its enterprise architecture communications plan that will be used to help business and IT management and staff develop a corporate model of customer service.

More recently, on September 5, the Secretary approved the initial version of the department's One VA enterprise architecture. VA officials describe the architecture as a top-down, business-focused document that provides

[10]Among the experts that VA consulted was John Zachman, author of "A Framework for Information Systems Architecture," referred to as the Zachman framework (*IBM Systems Journal*, vol. 26(3), 1987). This framework provides a common context for understanding a complex structure and enables communication among those involved in developing or changing the structure.

[11]Department of Veterans Affairs, *Department of Veterans Affairs (VA) Enterprise Architecture (EA)*, VA Directive 6051 (Washington, D.C.: July 12, 2002).

a blueprint for systematically defining and documenting the department's desired (target) environment. The document provides a high-level, overarching view of the department's "as is" enterprise business functions and key enabling functions.[12] VA's work to develop the "as is" view revealed the complexities of its baseline information systems, work processes, and supporting infrastructure. For example, it identified over 30 independently designed and operated data networks, over 200 independent external network connections, over 1,000 remote access system modem connections, and a total of 7,224 office automation servers that are currently part of the baseline environment.

The enterprise architecture document also incorporates high-level versions of a sequencing plan, technical reference model, and standards profile—all of which are critical to ensuring the complete development and implementation of the architecture. A sequencing plan serves as a systems migration roadmap to provide the agency with a step-by-step process for moving from the baseline to the target architecture. The technical reference model provides a knowledge base for a common conceptual framework, defines a common vocabulary and set of services and interfaces, and serves as a tool for the dissemination of technical information across the department. The standards profile, used in conjunction with the technical reference model, assists departmental components in coordinating the acquisition, development, and interoperability of systems to accomplish the department's enterprise architecture program goals.

Further, VA has integrated security practices into the initial version of its enterprise architecture. These security practices provide a high-level description of the baseline and target distributed systems architectures for major elements of the department's cyber security infrastructure.

Continued Commitment to Developing VA's Enterprise Architecture Is Essential

Even with notable progress, VA must nonetheless complete a number of additional actions to fully implement and effectively manage its enterprise architecture. With the Federal CIO Council's guide as a basis for analysis, table 1 illustrates the progress that the department has made since March

[12]Enterprise business functions are externally focused functions involving direct interactions with veterans across the enterprise, such as providing medical care benefits, vocational rehabilitation, and employment benefits. Key enabling functions are those necessary to support the enterprise business functions, such as eligibility and registration, and enable smooth operation of the overall enterprise both internally and externally.

in accomplishing key enterprise architecture process steps, along with examples of the various critical actions still required to successfully implement and sustain its enterprise architecture program.

Table 1: VA's Progress in Developing, Implementing, and Using an Enterprise Architecture as of September 2002

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Obtain executive buy-in and support			
Ensure agency head buy-in and support	√		
Issue executive enterprise architecture policy	√		
Obtain support from senior executive and business units	√		
Establish management structure and control			
Establish technical review committee	√		
Establish capital investment council		Drafted the Information Technology Integrated Management Guide, which lays out the integration of VA's EA, capital planning, investment, and project management functions Completed integration of its capital planning, investment, and project management functions, and uses it to evaluate IT projects	Finalize and issue the Information Technology Integrated Management Guide
Establish EA executive steering committee	√		
Appoint chief architect		Acting chief architect continues to fill position Recruitment effort for permanent chief architect continues; position expected to be filled in early 2003	Hire a chief architect with requisite core competencies
Establish EA program management office		Filled five positions in EA program management office Additional position advertisements being prepared, full staffing of office anticipated by the end of calendar year 2002	Fully staff the EA program management office with experienced architects to manage, control, and monitor development of the EA
Appoint key personnel for risk management, configuration management and quality assurance (QA)		Risk manager and configuration manager positions have not been filled, and VA does not plan to fill them The Enterprise Architecture Council will perform risk and configuration management and the Information Technology Board will perform QA functions	Ensure that adequate staffing occurs and functions are performed Establish an independent, objective entity to perform QA

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Establish enterprise architecture core team	√		
Develop EA marketing strategy and communications plan	√		
Develop EA program management plan			Develop and finalize a plan that will delineate actions to develop, use, and maintain the EA, including management control and oversight
Initiate development of enterprise architecture	√		
Define architecture process and approach			
Define intended use of architecture	√		
Define scope of architecture	√		
Determine depth of architecture	√		
Select appropriate EA products	√		
Select products that represent business of enterprise	√		
Select products that represent agency technical assets	√		
Evaluate and select framework	√		
Select EA tool set	√		
Develop baseline enterprise architecture			
Collect information that describes existing enterprise		Version 1.0 of VA's EA includes high-level descriptions of its baseline enterprise architecture business functions and key enabling functions from the planners' business owners' designers' and builders' viewpoints.	Continue development of the enterprise architecture to fully describe and document all current business functions and the technology infrastructure
Generate products and populate EA repository[b]		Repository established on VA's intranet Web site is populated with data on the planners' and owners' views of VA's architecture In FY 2003 VA plans to assess the need to develop a new repository and the contents of that repository	Complete population of the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models		Enterprise Architecture Council subject matter experts reviewed, validated, and refined models contained in version 1.0 of the enterprise architecture Council membership included representatives from VA's technical and business lines	Have subject matter experts continue to assess the enterprise architecture products for accuracy and completeness

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Develop target enterprise architecture			
Collect information that defines future business operations and supporting technology: strategic business objectives information needed to support business applications to provide information technology to support applications		Version 1.0 of VA's enterprise architecture contains high-level descriptions of VA's enterprise business functions and key enabling functions from the planners' and business owners' views of the Zachman framework	Continue to decompose and further define key elements of the target architecture
Generate products and populate EA repository		Repository established on VA's intranet Web site is populated with data on the planners' and owners' views of the VA architecture In FY 2003 VA plans to assess the need for another repository and the contents of that repository	Complete population of the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models		Subject matter expert review of version 1.0 of the enterprise architecture carried out by members of the Enterprise Architecture Council from VA's technical and business lines	Have subject matter experts continue to assess the enterprise architecture products for accuracy and completeness
Develop sequencing plan			
Identify gaps		July 8, 2002 sequencing plan contained in version 1.0 of EA provides a high-level overview of how VA will migrate from the current to the target architecture	Future version of the sequencing plan should identify gaps to assess the state of legacy systems, technology maturity, acquisition opportunities, and fiscal reality of the transition
Define and differentiate among legacy, migration, and new systems			Address all activities in this step
Plan migration			Address all activities in this step
Approve, publish, and disseminate EA products			Address all activities in this step
Use enterprise architecture			
Integrate EA with capital planning and investment control and systems life cycle processes		Drafted the Information Technology Integrated Management Guide, which lays out the integration of VA's EA, capital planning, investment, and project management functions Implemented the integrated capital planning, investment, and project management functions, and uses then to evaluate IT projects	Finalize and issue the Information Technology Integrated Management Guide

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Train personnel		Developing a project manager training curriculum Used the annual department CIO conference to conduct an overview of the department's EA effort	Ensure that members of all EA decision-making bodies are trained in the EA process, the relationship of the EA to the capital planning and investment control process, and the system life cycle; EA training should also be provided to current and future IT project managers
Establish enforcement processes and procedures		Published the following documents, which relate to enforcement of EA processes and procedures: • VA Directive 6051 • VA EA Strategy, Governance, & Implementation • One-VA EA Implementation Plan: FY 2002 • One-VA Enterprise Architecture (version 1.0)	Develop precise definitions and criteria for compliance as well as different levels of compliance
Define compliance criteria and consequences			Address all activities in this step
Set up integrated reviews			Address all activities in this step
Execute integrated process			Address all activities in this step
Initiate new and follow-up projects			Address all activities in this step
Prepare proposal			
Align project to EA			
Make investment decision			
Execute projects			Address all activities in this step
Manage and perform project development			
Evolve EA with program/project			
Assess progress			
Complete project			Address all activities in this step
Deliver product			
Assess architecture			
Evaluate results			
Consider other uses of EA			
Maintain enterprise architecture			Address all detailed activities in this step
Maintain EA as enterprise evolves			

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Reassess EA periodically			
Manage projects to reflect reality			
Ensure business direction and processes reflect operations			
Ensure current architecture reflects system evolution			
Evaluate legacy system maintenance requirements against sequencing plan			
Maintain sequencing plan as integrated program plan			
Continue to consider proposals for EA modifications			

[a]Chief Information Officer Council.

[b]A repository is an information system used to store and access architectural information, relationships among the information elements, and work products.

Source: GAO analysis.

As the table indicates, immediate attention still needs to be focused on acquiring a permanent chief architect to manage the development and maintenance of the enterprise architecture. Currently, the chief technology officer serves as the acting chief architect while the department recruits someone to fill the position on a permanent basis. According to the acting chief architect, VA anticipates filling the position in early 2003. The enterprise architecture program management office likewise needs to be fully staffed. As of September 6, 5 of the office's 16 positions had been filled. Officials expect this office to be fully staffed by the end of this year. Instituting a permanent chief architect with the requisite core competencies to lead the enterprise architecture development and fully staffing the enterprise architecture program office to support the effort, will provide vital components of management and oversight necessary for a successful enterprise architecture program.

Two quality assurance roles—those of risk manager and configuration manager—also still need to be filled. At the conclusion of our review, VA's Enterprise Architecture Council was performing risk and configuration management and its Information Technology Board was performing quality assurance functions. However, Federal CIO Council guidance recommends that the CIO make risk and configuration management the explicit responsibilities of individuals designated for those roles. The guide further recommends that the CIO establish an independent quality assurance function to evaluate the enterprise architecture.

VA must also still develop a program management plan to delineate how it will develop, use, and maintain the enterprise architecture. Such a plan is integral to providing definitive guidance for effectively managing the enterprise architecture program.

Beyond these actions, VA must continue to enhance the enterprise architecture that it has begun instituting. For example, additional work is needed to fully develop the baseline and target architectures to encompass all of the department's business functions, identify common areas of business, and eliminate duplication of processes across the organization through business process reengineering. As the initial version of the enterprise architecture notes, significant process duplication exists across the department. For example, VA identified eight different ways in which registration and eligibility are determined in the "as-is" (baseline) architecture. Nonetheless, although VA recognized opportunities for integrating and consolidating the department's duplicate processes and functions, its initial enterprise architecture document lacked any specific guidance on how and when consolidation and integration will take place.

Also, important to the success of an enterprise architecture effort is a fully-developed enterprise architecture repository.[13] Such a system serves to highlight information interdependencies and improves the understandability of information across an organization. It also helps to significantly streamline change control by establishing linkages among the information, facilitating impact analyses, and providing for ready evaluations of change proposals. Although VA's enterprise architecture repository contains information reflecting the views of its business planners and owners, the department still needs to completely populate the repository with data that describe the interrelationships among all information elements and work products. The acting chief architect stated that, in fiscal year 2003, the department will assess its need for a different system to serve as the EA repository.

As establishment of the enterprise architecture proceeds, VA also will need to further refine its sequencing plan to identify differences between baseline and target architectures and gaps in the process, and to assess the state of legacy, migration, and new systems, and budget priorities and constraints. In addition, the acting chief architect noted that the current

[13]A repository is an information system used to store and access architecture information, relationships among the information elements, and work products.

version of the technical reference model is generic and will require further development. Such customization is important in order to provide VA with consistent sets of service areas and interface categories and relationships used to address interoperability and open systems issues and serve as a basis for identifying, comparing, and selecting existing and emerging standards and their relationships. Such a document can also be used to organize infrastructure documentation.

According to VA officials, actions to refine and build upon the enterprise architecture are ongoing, and the department plans to issue an interim revision to the initial document within 4 to 6 months, and a completely new version by July 2003. The Enterprise Architecture Council will be responsible for developing these products. As the enterprise architecture management program moves forward, the department must ensure that it continues to sufficiently address and complete all critical process steps outlined in the federal CIO guidance within reasonable time frames. With enhanced management capabilities provided by an enterprise architecture framework, VA should be able to (1) better focus on the strategic use of emerging technologies to manage its information, (2) achieve economies of scale by providing mechanisms for sharing services across the department, and (3) expedite the integration of legacy, migration and new systems.

Information Security Continues to Require Top Management Attention

VA's information security continues to be an area of significant concern. The department relies extensively on computer systems and telecommunications networks to meet its mission of providing health care and benefits to veterans. VA's systems support many users, its networks are highly interconnected, and it is moving increasingly to more interactive, Web-based services to better meet the needs of its customers. Effectively securing these systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive medical information, and ensure the reliability of its financial data.

As this subcommittee is well aware, VA has faced long-standing challenges in achieving effective computer security across the department. Since 1998 we have reported on wide-ranging deficiencies in the department's

computer security controls.[14] Among the weaknesses highlighted was that VA had not established effective controls to prevent individuals from gaining unauthorized access to its systems and sensitive data. In addition, the department had not provided adequate physical security for its computer facilities, assigned duties in a manner that segregated incompatible functions, controlled changes to its operating systems, or updated and tested its disaster recovery plans. Similar weaknesses have been confirmed by VA's inspector general, as well as through the department's own assessments of its computer security controls in response to government information reform legislation.[15] As evidence, since September 2001, VA has self-reported approximately 27,000 control weaknesses related to physical and logical access, segregation of duties, system and application controls, and continuity of operations. As of August 31, 2002, according to VA, about half (14,000) of these weaknesses remained unresolved.

Contributing significantly to VA's computer security problems has been its lack of a fully implemented, comprehensive computer security management program—essential to managing risks to business operations that rely on its automated and highly interconnected systems. Our 1998 report on effective security management practices used by several leading public and private organizations[16] and a companion report on risk-based security approaches in 1999[17] identified key principles that can be used to establish a management framework for more effective information security programs. This framework, depicted in figure 3, points to five key areas of effective computer security program management—central security management, security policies and procedures, risk-based assessments, security awareness, and monitoring and evaluation. Leading organizations we examined applied these key principles to ensure that

[14]U.S. General Accounting Office, *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure*, GAO/AIMD-98-175 (Washington, D.C.: Sept. 23, 1998) and GAO-02-369T.

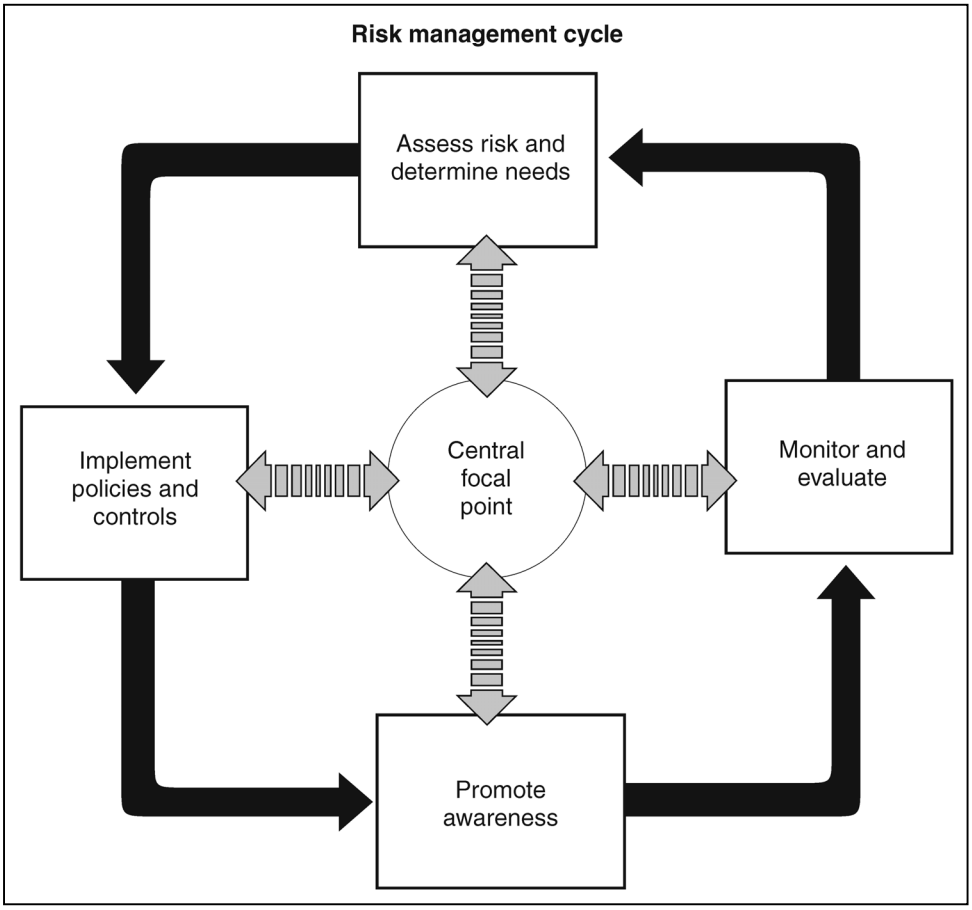
[15]The government information security reform provisions of the fiscal year 2001 Defense Authorization Act (P.L. 106-398) require annual agency program reviews and annual independent evaluations for both non-national security and national security information systems.

[16]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[17]U. S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D. C.: November 1999).

information security addressed risks on an ongoing basis. Further, these principles have been cited as useful guidelines for agencies by the Federal CIO Council and incorporated into the council's information security assessment framework,[18] intended for agency self-assessments.

Figure 3: Information Security Risk Management Framework



Source: GAO/AIMD-98-68.

When we testified before the subcommittee in March, VA had begun a number of actions to strengthen its overall computer security management posture. For example, the Secretary had instituted information security

[18]Chief Information Officers Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000).

standards for members of the department's senior executive service to provide greater management accountability for information security. In addition, VA's cyber security officer had organized his office to focus more directly on the critical elements of information security control that are defined in our information systems controls audit methodology.[19] The cyber security officer also had updated the department's security management plan, outlining actions for developing risk-based security assessments, improving the monitoring and testing of systems controls, and implementing departmentwide virus-detection software and intrusion-detection systems. The plan placed increased emphasis on centralizing key security functions that were previously decentralized or nonexistent, including virus detection, systems certification and accreditation, network management, configuration management, and incident and audit analysis.

Nonetheless, while VA had completed a number of important steps, its security management program continued to lack essential elements required for protecting the department's computer systems and networks from unnecessary exposure to vulnerabilities and risks. For example, while the department had begun to develop an inventory of known security weaknesses, it had not instituted a comprehensive, centrally managed process that would enable it to identify, track, and analyze all computer security weaknesses. Further, the updated security management plan did not articulate critical actions that VA would need to take to correct specific control weaknesses or time frames for completing key actions.

Progress Continues, but Actions Still Needed to Achieve a Comprehensive Security Management Program

Since March, the department has taken important steps to further strengthen its computer security management program. For example, the cyber security officer has updated and expanded the department's information security policies and procedures, placing increased emphasis on better securing and overseeing the department's computer environment. More recently, as discussed earlier, VA's realignment of its information technology resources placed administration and field office security functions more directly under the oversight of the department's CIO.

[19]U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

VA has also acted to help provide a more solid foundation for detecting, reporting, and responding to security incidents. For example, it has contracted to acquire an expanded departmentwide incident response and analysis capability, to include enhanced security monitoring and detection. Further, it has enhanced its computer virus detection program by providing technical training to operational staff and distributing antivirus patches for known viruses to affected systems. In addition, VA has initiated a multiyear project intended to consolidate, protect, and centrally manage external connections to its critical financial, medical, and benefits systems. This project, with full implementation planned for September 2004, is expected to reduce the approximately 200 external computer network connections that the department now relies on to about 10. By reducing these connections, VA should be better positioned to effectively reduce its risk of unauthorized access to its critical systems.

As was the case last March, however, VA's actions have not yet been sufficient to fully implement all of the key elements of a comprehensive computer security management program. In assessing the department's recent corrective actions relative to our information security risk management framework, VA still needs to accomplish a number of critical tasks that are essential to successfully achieving a comprehensive and effective computer security management program. Table 2 summarizes the steps that VA still needs to accomplish in order to fully implement a comprehensive program.

Table 2: Actions Needed to Ensure a Comprehensive Computer Security Management Program

Important elements of a computer security management program[a]	Actions needed as of March 2002	Actions VA has taken since March 2002	Actions still needed
Central security management function to guide and oversee compliance with established policies and procedures and review effectiveness of the security environment	Ensure that full-time security officers or staff with primary duty for security are assigned to information security officer (ISO) positions and clearly define their roles and responsibilities Develop guidance to ensure authority and independence of security officers Develop policies and procedures to ensure departmentwide coordination of security functions	Established a tracking mechanism to identify security officers and the systems under their respective purview at each location VA Secretary centralized the department's IT program, including authority, personnel, and funding, in the Office of the Chief Information Officer	Ensure that full-time security officers or staff with primary duty for security are assigned to all ISO positions and clearly define their roles and responsibilities In conjunction with VA's centralization of the IT program, develop policy and guidance to ensure (1) authority and independence for security officers and (2) departmentwide coordination of security functions
Security policies and procedures that govern a complete computer security program and integrate all security aspects of an	Refocus department policy to address security from an interconnected VA systems environment perspective in addition to that of individual	Developed policies to address external connections and standards for public key infrastructure authentication	Develop specific policy to address security interconnectivity of all internal and external VA systems Develop and implement technical

Important elements of a computer security management program[a]	Actions needed as of March 2002	Actions VA has taken since March 2002	Actions still needed
organization's environment, including local area networks, wide area networks, and mainframe security	systems Develop and implement technical security standards for mainframe and other systems and security software		security standards for mainframe and other systems and security software
Periodic risk assessments to assist management in making decisions on necessary controls to help ensure that security resources are effectively distributed to minimize potential loss	Include best minimum standards or guidance for performing risk assessments in methodology Develop guidance for determining when an event is a significant change and explaining the level of risk assessment required for these system changes		Include best minimum standards or guidance for performing risk assessments in methodology Develop guidance for determining when an event is a significant change and explaining the level of risk assessment required for these system changes
Security awareness to educate users about current information security risks, policies, and procedures	Establish a process to ensure program compliance		Establish a process to ensure program compliance
Monitoring and evaluating computer controls to ensure their effectiveness, improve them, and oversee compliance	Develop specific requirements for conducting a compliance review program Develop an ongoing program for testing controls to include assessments of both internal and external access to VA systems; expand current tests to identify unauthorized or vulnerable external connections to VA's network Establish a process for tracking the status of security weaknesses, corrective actions taken, and independent validation of the corrective actions Develop a process for routinely analyzing the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve security Develop a proactive security incident response program to monitor user access for unusual or suspicious activity	Initiated a multiyear project to consolidate, protect, and centrally manage external connections to VA systems Developed a process for tracking the status of computer security weaknesses and corrective actions taken Developed an ad hoc approach for identifying computer control weaknesses for review Awarded contract for an expanded security incident response and analysis program to include security monitoring and detection capability for external user access activities Enhanced computer virus detection program by providing technical training to operational staff and distributing antivirus patches	Develop specific requirements for conducting a compliance review program Develop an ongoing program for testing controls to include assessments of both internal and external access to VA systems; expand current tests to identify unauthorized or vulnerable external connections to VA's network Develop a process to independently validate corrective actions taken Develop a process that emphasizes routinely analyzing the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve security Develop a proactive security incident response program to provide for both internal and external monitoring of user access to identify unusual or suspicious activities

[a]GAO/AIMD-98-68.

Source: GAO.

The department's critical remaining actions include routinely monitoring and evaluating the effectiveness of security policies and controls and acting to address identified weaknesses. These tasks aid organizations in cost effectively managing their information security risks rather than reacting to individual problems after a violation has been detected. We have previously recommended that VA establish a program involving ongoing monitoring and evaluation to ensure the effectiveness of its computer control environment. An effective program framework would include a description of the scope and level of testing to be performed, specific control areas to be tested, the frequency of testing, and the identity of responsible VA units. In addition, testing and evaluation would include penetration tests and reviews of the computer network, as well as compliance reviews of all computer control areas, including logical and physical access controls; service continuity tests; and system and application integrity and change controls performed on a scheduled basis.

VA has begun placing greater emphasis on controlling its security risks; however, its current framework does not yet include some of the essential elements required to achieve a formal program for monitoring and evaluating computer controls. For example, while the department has conducted some tests of its control environment, including penetration tests and reviews of its computer network, this effort has largely been performed in an ad hoc manner, rather than as part of a formal, ongoing program. Further, while VA has established a departmental process for assessing computer controls, the process relies on VA's offices to self-report computer control weaknesses, with no independent validation component to ensure the accuracy of reporting.

Similarly, an effective computer security management program should include a process for ensuring that remedial action is taken to address significant deficiencies and that it provides steps to analyze weaknesses reported for identifiable trends and vulnerabilities, and to apply appropriate countermeasures as needed. Although VA has established a system for tracking corrective actions, it has not developed a process for independently validating or reviewing the appropriateness of the corrective actions taken. Further, the department currently lacks a process to routinely analyze the weaknesses reported, limiting its effectiveness at identifying systemic problems that could adversely affect critical veterans information systems departmentwide.

Finally, although VA has developed a framework for addressing departmentwide computer security, it has not yet established a mechanism for collecting and tracking performance data, ensuring management

review when appropriate, or providing for independent validation of program deliverables. Until it addresses all key elements of a comprehensive computer security management program and develops a process for managing the department's security plan, VA will not have full assurance that its financial information and sensitive medical records are adequately protected from unauthorized disclosure, misuse, or destruction.

VBA Remains Far from Full Implementation of the VETSNET Compensation and Pension Replacement System

Mr. Chairman, we continue to be concerned about the slow progress that VBA is making in implementing the VETSNET compensation and pension replacement system. As you know, VBA currently relies on its aging Benefits Delivery Network to deliver over 3.5 million benefits payments to veterans and their dependents each month.[20] The compensation and pension replacement effort grew out of an initiative that VBA undertook in 1986 to replace its outdated BDN and modernize its compensation and pension, education, and vocational rehabilitation benefits payment systems. After several false starts and approximately $300 million spent on the overall modernization, the administration revised its strategy in 1996 and began focusing on modernizing the compensation and pension (C&P) payment system.

VBA has now been working on the C&P replacement initiative for more than 6 years, but continues to be far from full implementation of the new payment system. As we reported last March, long-standing, fundamental deficiencies in VBA's management of the project hindered successful development and implementation of the system. For example, the initiative was proceeding without a project manager, and VBA had not obtained essential field office support for the new software being developed. In addition, users' requirements for the new system had not yet been assessed or validated to ensure that VETSNET would meet business needs; and testing of the system's functional business capability, as well as end-to-end testing to ensure that accurate payments would be delivered, still needed to be completed. Finally, VBA had not developed an integrated project plan to guide its transition from BDN to the new system.

This past June, we recommended that, before approving any new funding for the replacement system, the Secretary should ensure that actions are taken to address our long-standing concerns about VBA's development

[20]Parts of the Benefits Delivery Network were developed in the 1960s.

and implementation of the system. These recommended actions included (1) appointing a project manager to direct the development of an action plan for, and oversee the complete analysis of, the current system replacement effort; (2) finalizing and approving a revised C&P replacement strategy based on results of the analysis and implementing an integrated project plan; (3) developing an action plan to move VBA from the current to the replacement system; and (4) developing an action plan to ensure that BDN will be available to continue accurately processing benefits payments until the new system is deployed.[21] The department concurred with our recommendations, and stated that actions were either under way or planned to implement them.

Actions Taken in Recent Months

Since our March testimony and subsequent recommendations, VBA has acted to further its development and implementation of the C&P replacement system. Among these actions VBA began recruiting a full-time project manager in June, and, according to the deputy CIO for VBA, expects to fill this position by the end of this month. In addition, to obtain field office and program support, in late March VBA formalized an implementation charter that established a VETSNET executive board and a project control board.[22] These entities are expected to provide decision support and oversee progress on the implementation. VBA has also begun revalidating functional business requirements for the new system. Its July 10, 2002 status report called for validating the majority of its requirements by the end of this month, and to complete all requirements validation by January 2003. The report also identified actions needed to transition VBA from the current to the replacement system. Further, in July VBA hired a contractor to obtain support for testing the VETSNET system applications. The contractor has been tasked with conducting functional, integration, and linkage testing, as well as software quality assurance for each release of the system applications.

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

[22]The executive board meets monthly and consists of VBA's chief financial officer, deputy chief information officer, director of compensation and pension service, and director of field operations. The project control board meets weekly and comprises representatives from the Office of Information Management, Compensation and Pension Service, Office of Resource Management, Field Operations, and the Program Analysis and Integrity Office. It is codirected by a business project manager and a technical project manager.

Much Work Remains

Nonetheless, VBA still has significant work to accomplish, and completing its implementation of the new system could take several years. All but one of the software applications comprising the new system still need to be fully deployed or developed, and VBA is currently processing only nine benefits claims using its new software products.[23] As described in VA's August 2002 Compensation and Pension Replacement System Capital Asset Plan, the C&P replacement strategy incorporates six software applications: (1) Share, (2) Modern Award Processing - Development, (3) Rating Board Automation 2000, (4) Award Processing, (5) Finance and Accounting System, and (6) Correspondence. These applications are being designed to support the processing of initial benefits claims for service-connected disabilities, as shown in table 3.

Table 3: C&P Replacement System's Support of Initial Disability Claims Processing

C&P replacement system software application	Initial disability claims processing and benefit payment functions
Share (establishment)	Establish the claim—regional office enters basic information provided by the veteran into a computer system and sets up a claim file folder
Modern Award Processing – Development (MAP-D)	Develop the claim—regional office reviews the claim file folder for military service and medical information, requests and obtains missing information, and assesses information to determine basic eligibility
Rating Board Automation 2000 (RBA 2000)[a]	Rate the claim—regional office analyzes the veteran's service records and service and private medical records and determines the veteran's level of disability
Award Processing (AWARD)	Authorize the claim—regional office reviews previous work on the claim, approves the initiation of benefit payments, and notifies the veteran of the decision
Finance and Accounting System (FAS)	Pay beneficiary—regional office enters data into computer system to generate and make payment to veterans
Correspondence	Notify veteran—regional office sends letters informing veterans of the status of actions to process their claims

[a]The Search and Participant Profile application is used in conjunction with RBA 2000 and pulls information from the corporate database when reopened claims are rated and is transparent to the user. Until recently, this application had been counted separately.

Source: GAO analysis.

VBA still has numerous tasks to accomplish before these software applications can be fully implemented. Although, last year, the administration implemented its rating board automation tool (RBA 2000), it will not require all of its regional offices to use this software until July 2003. In addition, our recent follow-up work determined that two of the

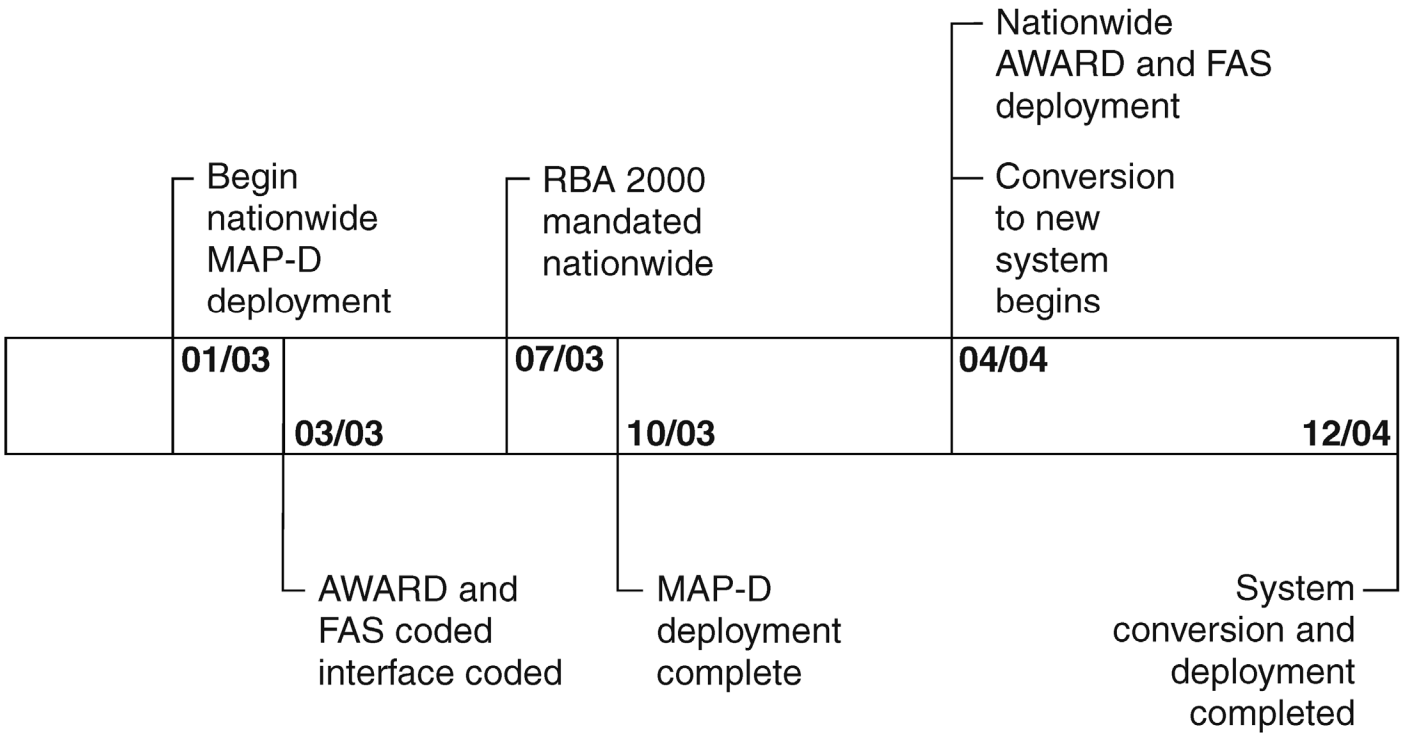
[23]As part of a pilot test in February 2001, VBA began processing ten original benefits claims using its new software. However, according to VBA, one veteran included in the pilot moved to West Virginia, and his payment is now being delivered by the BDN.

software products continue to be in various stages of deployment. Specifically, among the 57 regional offices that are expected to benefit from the replacement system, only 6 are currently using Share to establish a claim; VBA still needs to implement the tool in the 51 other regional offices. In addition, only two regional offices—Salt Lake and Little Rock—have pilot-tested and are currently using MAP-D to assist in the development of most compensation claims. VBA still needs to implement this tool in 55 other regional offices. Full implementation is currently estimated for October 2003.

Further, three software applications—AWARD, FAS, and Correspondence—continue to require development. According to VBA officials, when implemented, AWARD will record award decisions and generate, authorize, and validate on-line awards for veterans and interface with Correspondence to develop the notification letter for the veteran. FAS will provide the accounting benefits payments functions and will include an interface with the Department of the Treasury.

VBA expects to complete software coding for AWARD and FAS by March 2003. Based on its most recent estimates, it expects to begin nationwide deployment of the two systems in April 2004. Once these activities are accomplished, VBA plans to begin its conversion to the new system, with a completion date currently set for December 2004. Figure 4 depicts VBA's current time line for the full implementation of the system.

Figure 4: VBA's Time Line for Completing and Implementing the Compensation & Pension Replacement Payment System (as of July 2002)



Source: Veterans Benefits Administration.

Maintaining Benefits Delivery Network Operations Is Critical to Ensuring Continued Payments to Veterans

Given its current schedule for implementing the C&P replacement system, VBA will have to continue relying on BDN to deliver compensation and pension benefits payments until at least the beginning of 2005. However, with parts of this system nearing 40 years old, without additional maintenance, BDN's capability to continue accurately processing benefits payments is uncertain. Our concerns have been substantiated by the VA claims processing task force, which in its October 2001 report warned that the system's operations and support were approaching a critical stage and that its performance could potentially degrade and eventually cease.[24]

[24]The claims processing task force was formed in May 2001, when the Secretary of Veterans Affairs asked a group of individuals with significant experience to assess and critique VBA's compensation and pension organization, management, and processes, and to develop recommendations to significantly improve VBA's ability to process veterans' claims for disability compensation and pensions.

Since March, VBA has taken steps to help ensure that BDN can be sustained and remains capable of making prompt, uninterrupted payments to veterans. For example, VBA has (1) completed an upgrade of BDN hardware, (2) hired 11 new staff members dedicated to BDN operations, and (3) successfully tested a contingency plan. Further, according to VBA's deputy CIO, the administration has developed an action plan outlining strategies for keeping BDN operational until the replacement system is implemented. Nonetheless, the risks associated with continual reliance on BDN remain—one of the system's software applications (database monitor software) is no longer supported by the vendor, nor is it used by any other customer.

Government Computer-Based Patient Record Initiative Has Changed Name, Goals, Strategy

Finally, Mr. Chairman, I would like to provide updated information on VA's progress, in conjunction with the Department of Defense (DOD) and the Indian Health Service (IHS), in achieving the ability to share patient health care data as part of the government computer-based patient record (GCPR) initiative. As you know, the GCPR project was developed in 1998 out of VA and DOD discussions about ways to share data in their health information systems and from efforts to create electronic records for active duty personnel and veterans. IHS became involved because of its experience in population-based research and its long-standing relationship with VA in caring for the Indian veteran population, as well as its desire to improve the exchange of information among its facilities.

GCPR was originally envisioned to serve as an electronic interface that would allow physicians and other authorized users at VA, DOD, and IHS health facilities to access data from any of the other agencies' health facilities by serving as an electronic interface among their health information systems. The interface was expected to compile requested patient information in a temporary, "virtual" record that could be displayed on a user's computer screen.

Last March we expressed concerns about the progress that VA, DOD, and IHS had made toward implementing GCPR. We testified that the project continued to operate without clear lines of authority or a lead entity responsible for final decision-making. The project also continued to move forward without comprehensive and coordinated plans, including an agreed-upon mission and clear goals, objectives, and performance

measures. These concerns were originally reported in April 2001,[25] when we recommended that the participating agencies (1) designate a lead entity with final decision-making authority and establish a clear line of authority for the GCPR project, and (2) create comprehensive and coordinated plans that included an agreed-upon mission and clear goals, objectives, and performance measures, to ensure that the agencies can share comprehensive, meaningful, accurate, and secure patient health care data. VA, DOD, and IHS all agreed with our findings and recommendations.

Our March testimony also noted that the scope of the GCPR initiative had been narrowed from its original objectives and that the participating agencies had announced a revised strategy that was considerably less encompassing than the project was originally intended to be. Specifically, rather than serve as an interface to allow data sharing across the three agencies' disparate systems, as originally envisioned, a first (near-term) phase of the revised strategy had called only for a one-way transfer of data from DOD's current health care information system to a separate database that VA hospitals could access.

Subsequent phases of the effort that were to further expand GCPR's capabilities had also been revised. A second phase that would have enabled information exchange among all three agencies had been re-scoped to enable only a bilateral read-only exchange of data between VA and IHS. Plans for a third phase involving the expansion of GCPR's capabilities to public and private national health information standards groups were no longer being considered for the project, and there were no plans for DOD to receive data from VA.

GCPR Is Proceeding under a New Name and Strategy

In May, VA and DOD proceeded with implementing the revised strategy. It finalized a memorandum of agreement that designated VA as the lead entity in implementing the project and formally renamed the project the Federal Health Information Exchange (FHIE) Program. According to program officials, FHIE is now a joint effort between DOD and VA that will enable the exchange of health care information in two phases. The first phase, or near-term solution, is to enable the one-way transfer of data from

[25]U.S. General Accounting Office, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing*, GAO-01-459 (Washington, D.C.: Apr. 30, 2001).

DOD's existing health care information system to a separate database that VA hospitals can access. Nationwide deployment and implementation of the first phase began in late May of this year, and was completed in mid-July.

FHIE was built to interface with VA's and DOD's existing systems. Specifically, electronic data from separated service members contained in DOD's Military Health System Composite Health Care System are transmitted to VA's FHIE repository, which can then be accessed through the Computerized Patient Record System (CPRS) in VA's Veterans Health Information Systems and Technology Architecture (VISTA). Clinicians are able to access and display the data through CPRS remote data views.[26] The data currently available for transfer include demographic[27] and certain clinical information, such as laboratory results, outpatient pharmacy data, and radiology reports on service members that have separated from DOD.

The final phase of the near-term solution is anticipated to begin this October. According to VA and DOD officials, this phase is intended to broaden the base of health information available to VA clinicians through the transfer of additional health information on separated service members. This additional information is expected to consist of discharge summaries;[28] allergy information; admissions, disposition, and transfer information; and consultation results that include referring physicians and physical findings. Completion of this final phase of FHIE is scheduled for September 2003. VA and DOD have budgeted $12 million in fiscal year 2003 ($6 million for each agency) to cover completion and maintenance of the near-term effort.

VA and DOD Report Success in Implementing the First Phase of FHIE

FHIE is currently available to all VA medical centers, and according to program officials, is showing positive results. The officials stated that, presently, the FHIE repository contains data on almost 2 million unique patients. This includes clinical data on over 1 million service personnel who separated between 1987 and 2001. The data consist of over 14 million

[26]The CPRS remote data views is an application that allows authorized users to access patient health care data from any VA medical facility.

[27]The demographic information consists of patient name, DOD eligibility category, Social Security number, address, date of birth, religion, primary language, sex, race, and marital status.

[28]Discharge summaries will include inpatient histories, diagnoses, and procedures.

lab messages, almost 14 million pharmacy messages, and over 2 million radiology messages.

Program officials stated that the quick retrieval and readability of data contained in the FHIE repository has begun providing valuable support to VA clinicians. They stated that FHIE is capable of accommodating up to 800 queries per hour, with an average response rate of 14 seconds per query. For the week beginning July 29, 2002, VA clinicians made 287 authorized queries to the database. In addition, when a clinician at a VA medical facility retrieves the data transmitted from DOD, the data appear in the same format as the data captured in CPRS, further facilitating its use. During a demonstration of the data retrieval capability, a clinician at VA's Washington, D.C., medical center told us that the information provided through FHIE has proven particularly valuable for treating emergency room and first-time patients. He added that additional data anticipated from the second phase of FHIE should prove to be even more valuable.

VA and DOD Developing Interoperable Health Systems

Beyond FHIE, VA and DOD have envisioned a long-term strategy involving the two-way exchange of clinical information. This initiative has been termed HealthePeople (Federal). According to VHA's CIO and the Military Health System CIO, VA and DOD are jointly implementing a plan that will result in computerized health record systems that ensure interoperability between DOD's Composite Health Care System II and VA's HealtheVet VISTA to achieve the sharing of secure health data required by their health care providers.[29] In order to accomplish this objective, the two agencies intend to standardize health and related data, communications, security, and software applications where appropriate. As part of HealthePeople (Federal), IHS is also expected to be actively involved in helping to develop national standards and compatible software applications to further the standardization of data, communications, and security for health information systems. When our review concluded, VA and DOD had just begun this initiative, with a focus on addressing the standardization issue. At that time, they anticipated implementing this exchange of clinical information by the end of 2005.

[29]Both of these systems are currently under development.

In summary, Mr. Chairman, VA continues to make important progress toward improving its management of information technology, with the attention and support of its executive leadership contributing significantly to ongoing actions to improve key areas of IT performance. The restructuring of responsibility and accountability directly to the CIO is a particularly important step—one that could set the stage for VA truly achieving its One-VA vision. In addition, actions aimed at further developing the department's enterprise architecture and improving computer security management continue to help solidify the IT foundation necessary

to guide VA's development and protection of critical information systems and data that are vital to its mission. Finally, although under a revised, scaled-down initiative, VA and DOD have made some progress in achieving the capability to share health care data on military personnel and veterans. Yet, challenges remain. Ensuring that the enterprise architecture will be fully implemented and sustained beyond the current leadership necessitates that the department establish a program management structure to guide and oversee this critical initiative. Completing its comprehensive computer security management program is also essential to ensure that the department can effectively safeguard its assets and sensitive medical information. Further, the urgency that VA faces in replacing its aging BDN continues to grow, while much must be accomplished before full implementation of the compensation and pension replacement system. Instituting the necessary processes and controls to guide VA's information technology programs and investments will be vital to ensuring that the department does not fall short of its goals of enhancing operational efficiency and, ultimately, improving service delivery to our nation's veterans.

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) 512-6253 or by e-mail at willemssenj@gao.gov. Individuals making key contributions to this testimony include Nabajyoti Barkakati, Nicole Carpenter, Kristi Dorsey, David W. Irvin, Min S. Lee, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, and Charles M. Vrabel.