Ms. Linda Koontz, Director of Information Management for the Government Accounting Office

Mr. Chairman and Members of the Committee:

Thank you for inviting us to take part in your discussion of the information technology organization at the Department of Veterans Affairs (VA) and the role of the Chief Information Officer (CIO). In carrying out its mission of serving our nation's veterans, the department relies heavily on information technology, for which it is requesting about $2.1 billion in funding for fiscal year 2006. The CIO will play a vital role in ensuring that this money is well spent and that information technology is managed effectively. As we have previously reported, an effective CIO can make a significant difference in building the institutional capacity that is needed to improve an agency's ability to manage information and technology and thus enhance program performance.

At your request, we will discuss the role of CIOs in the federal government, present for comparison the results of our study of private-sector CIOs, and provide a historical perspective on the roles and responsibilities of VA's CIO.

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

Results in Brief

Since the Clinger-Cohen act established the CIO position in 1996, federal CIOs have played a central role in managing information and technology within federal agencies. According to CIOs at major departments and agencies, they generally held wide responsibilities and reported to their agency heads or other top level managers. In general, CIOs reported that they were responsible for key information and technology management areas; for example, all the CIOs were responsible for five key areas (capital planning and investment management, information security, IT human capital, strategic planning for information technology and information resource management, and enterprise architecture). In carrying out these responsibilities, the tenure of federal CIOs was often less than the length of time that some experts consider necessary for them to be effective and implement changes: the median tenure was about 2 years, and the most common response regarding time required to be effective was 3 to 5 years. In contrast, CIOs were generally helped in carrying out their responsibilities by the background and experience they brought to the job. Although their background was varied, most had background in information technology (IT) or related fields, many having previously served as CIOs; many also had business knowledge related to their agencies, having previously worked either at the agency or in an area related to its mission. Other factors that help CIOs meet their responsibilities effectively are described in guidance that we have issued; key among these are (1) being supported by senior executives who recognize the importance to their missions of IT and an effective CIO; (2) playing an influential role in applying IT to business needs; and (3) being able to structure their organizations appropriately. At the same time, CIOs cited several challenges, of which the two most frequently mentioned were implementing effective IT management and obtaining sufficient and relevant resources.

Private-sector CIOs reported responsibilities, challenges, and approaches to information and technology governance that are similar but not identical to those of their federal counterparts. Most of the private-sector CIOs we contacted had either sole or shared responsibility for the key management areas we explored, which corresponded to those that we reported on in our federal agency review. Among the areas in which most of the private-sector CIOs had or shared responsibility, 18 or more of the 20 we contacted cited five information and technology management areas (capital planning and investment management, information security, human capital for managing information resources, systems acquisition, and e-commerce); the first three of these were also responsibilities of all federal CIOs, and the last two were responsibilities of 90 percent of federal CIOs. The challenges cited by the private-sector CIOs were also similar to those cited by federal CIOs. Both private-sector and federal CIOs noted improving various IT management processes (e.g., IT investment decision making), developing IT leadership and skills, working with enterprise architectures, and ensuring the security of systems. To manage their IT, the private-sector companies used both centralized and decentralized organizational structures: in some, authority is centralized in the CIO's office, while in others, it is decentralized in the business units, depending on other events in the company such as strategic realignments and acquisitions. Most of the private-sector companies had executive committees with authority and responsibility for governing major IT investments. Many private-sector CIOs also told us that they were making efforts to move toward common business processes, such as by instituting cross-organizational teams to work on developing enterprisewide systems and standards.

With regard to VA, both the CIO position and IT management have received increased management attention over time. After going for 2½ years after the passage of the Clinger-Cohen Act without a CIO, followed by 2 years with an executive whose time was divided among CIO and other major duties, and then 1 year with an acting CIO, the department appointed a full-time permanent CIO in August 2001. Since then, the department proposed further strengthening the position and centralizing IT management, recognizing that aspects of its computing environment were particularly challenging and required substantial management attention. In particular, the department's information systems and services were highly decentralized, and a large proportion of the department's IT budget was controlled by the VA's administrations and staff offices. To address these challenges, the Secretary issued a memo in 2002 announcing that IT functions, programs, and funding would be centralized under the department-level CIO. Although we have not reviewed the current status of this proposed realignment or VA's current organizational structure, it remains our view that the proposal held promise for improving IT accountability and enabling the department to accomplish its mission. The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively account for and manage its approximately $2.1 billion in planned IT spending.

Background

VA comprises three major components: the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration (NCA). VA's mission is summed up in its mission statement, a quotation from Abraham Lincoln: 'to care for him who shall have borne the battle and for his widow and his orphan.' VA carries out this mission by providing benefits and other services to veterans and dependents.

The department's vision is to be a more customer-focused organization, functioning as 'One VA.' This vision stemmed from the recognition that veterans think of VA as a single entity, but often encountered a confusing, bureaucratic maze of uncoordinated programs that put them through repetitive and frustrating administrative procedures and delays. The 'One VA' vision is to create versatile new ways for veterans to obtain services and information by streamlining interactions with customers and integrating IT resources to enable VA employees to help customers more quickly and effectively. This vision will require modifying or replacing separate information systems with integrated systems using common standards to share information across VA programs and with external partner organizations, such as the Department of Defense.

Accordingly, effective management of its IT programs is vital to VA's successful achievement of its vision and mission.

Table 1 shows a breakdown of VA's approximately $2.1 billion IT budget request for fiscal year 2006. Of the total, VHA accounted for approximately $1.8 billion, VBA approximately $150 million, and NCA approximately $11 million. The remaining $84 million was designated for the department level.

Table 1: Breakdown of VA's Fiscal Year 2006 Information Technology Budget Request (in millions)

Organization	Request	
VHA	$1835	88%
VBA	150	7%
NCA	11	<1%
Department	84	4%
Total	$2080	

Source: GAO analysis of VA data.

CIO Plays Major Role in Federal IT Management

The Congress has long recognized that IT has the potential to enable federal agencies to accomplish their missions more quickly, effectively, and economically. However, fully exploiting this potential presents challenges to agencies. Despite substantial IT investments, the federal government's management of information resources has produced mixed results. One of the ways in which the Congress has addressed this issue was to establish the CIO position; an agency's CIO is to serve as the focal point for information and technology management within an agency.

In 1996, the Clinger-Cohen Act established the position of agency CIO and specified responsibilities for this position. Among these responsibilities, the act required that the CIOs in the 24 major departments and agencies have information resources management (IRM) as their 'primary duty.'

The Congress has mandated that CIOs should play a key leadership role in ensuring that agencies manage their information functions in a coordinated and integrated fashion in order to improve the efficiency and effectiveness of government programs and operations.

CIO Responsibilities and Reporting Relationships

CIOs have responsibilities that can contribute significantly to the successful implementation of information systems and processes. In July 2004, we reported on CIO roles, responsibilities, and challenges (among other things) at 27 major agencies. For this work, we identified major areas of CIO responsibilities that were either statutory requirements or critical to effective information and technology management. Altogether, we identified the 13 areas shown in table 2.

Table 2: Major Areas of CIO Responsibility

Area of responsibility	Description	Applicable laws
IT capital planning and investment management	Planning and management of IT capital investments	44 U.S.C. 3506(h), 40 U.S.C. 11312 & 11313
Enterprise architecturea	Developing and maintaining the enterprise architecture defining the agency's mission and the information and IT needed to perform it	OMB guidance
Information security	Ensuring agency compliance with the requirement to protect information and systems	44 U.S.C. 3506(g) and 3544(a)(3)
IT/IRM strategic planning	Performing strategic planning for all information and information	

technology management functions 44 U.S.C. 3506(b)(2)

IT/IRM human capital Helping agency meet IT/IRM workforce needs 44 U.S.C. 3506(b), 40 U.S.C. 11315(c)

E-government initiativesa Supporting initiatives to use IT to improve government services to the public and internal operations 44 U.S.C. 3506(h)(3), E-Government Act of 2002, other laws and guidance

Systems acquisition, development, and integrationa Controlling the acquisition, development, and integration of IT systems 44 U.S.C. 3506(h)(5), 40 U.S.C. 11312

Information collection/paperwork reduction Reviewing proposals for agency information collections to maximize their utility and minimize public paperwork burden 44 U.S.C. 3506(c)

Records management Ensuring that agency implements and enforces records management policies and procedures under the Federal Records Act 44 U.S.C. 3506(f)

Information disseminationb Ensuring that information dissemination activities meet policy goals such as timely and equitable public access to information 44 U.S.C. 3506(d)

Information disclosureb Ensuring appropriate information access under the Freedom of Information Act 44 U.S.C. 3506(g)

Privacy Ensuring agency compliance with the Privacy Act and related laws 44 U.S.C. 3506(g)

Statistical policy and coordination Performing statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes 44 U.S.C. 3506(e)

Source: GAO analysis.

aThree areas of responsibility?enterprise architecture; systems acquisition, development, and integration; and e-government initiatives?are not assigned to CIOs by statute; they are assigned to the agency heads by law or guidance. However, in virtually all agencies, the agency heads have delegated these areas of responsibility to their CIOs.

b For our later private-sector study, we combined Information dissemination and Information disclosure into a single function in order to increase these functions' relevance for private-sector CIOs.

According to our report, CIOs were generally responsible for the key information and technology management areas shown in the table, although not all CIOs were completely responsible for all areas. For example:

- All the CIOs were responsible for the first five areas in the table (capital planning and investment management, enterprise architecture, information security, IT/IRM strategic planning, and IT/IRM human capital).
- More than half had responsibility for six additional areas (major e-government initiatives, systems acquisition, information collection/paperwork reduction, records management, information dissemination, and privacy).
- Fewer than half were responsible for two areas (information disclosure and statistics).

It was common for CIOs to share responsibility for certain functions, and in some cases responsibilities were assigned to other offices. For example, systems acquisition responsibility could be shared among the CIO and other officials, such as a procurement executive or program executive; disclosure could be assigned to general counsel and public affairs, while statistical policy could be assigned to offices that deal with the agency's data analysis. Nevertheless, even for areas of responsibility that were not assigned to CIOs, agency CIOs generally reported that they contributed to the successful execution of the agency's overall responsibilities in that area.

In carrying out their responsibilities, CIOs generally reported to their agency heads. For 19 of the agencies in our review, the CIOs stated that they had this reporting relationship. In the other 8 agencies, the CIOs stated that they reported instead to another senior official, such as a deputy secretary, under secretary, or assistant secretary. In addition, 8 of the 19 CIOs who said they had a direct reporting relationship with the agency head noted that they also reported to another senior executive, usually the deputy secretary or under secretary for management, on an operational basis. According to members of our Executive Council on Information Management and Technology, what is most critical is for the CIO to report to a top level official.

Tenure and Backgrounds of CIOs

Federal CIOs often remained in their positions for less than the length of time that some experts consider necessary for them to be effective and implement changes. At the major departments and agencies included in our review, the median time in the position of permanent CIOs whose time in office had been completed was about 23 months. For career CIOs, the median was 32 months; the median for political appointees was 19 months. To the question of how long a CIO needed to stay in office to be effective, the most common response of the CIOs (and former agency IT executives whom we consulted) was 3 to 5 years. Between February 10, l996, and March 1, 2004, only about 35 percent of the permanent CIOs who had completed their time in office reportedly had stayed in office for a minimum of 3 years. The gap between actual time in office and the time needed to be effective is consistent with the view of many agency CIOs that the turnover rate was high, and that this rate was influenced by the political environment, the pay differentials between the public and private sectors, and the challenges that CIOs face.

In contrast, the CIOs at the 27 agencies were generally helped in carrying out their responsibilities by the background and experience they brought to the job. The background of the CIOs varied in that they had previously worked in the government, the private sector, or academia, and they had a mix of technical and management experience. However, virtually all had work experience or educational backgrounds in IT or IT-related fields; 12 agency CIOs had previously served in a CIO or deputy CIO capacity. Moreover, most of the them had business knowledge related to their agencies because they had previously worked at the agency or had worked in an area related to the agency's mission.

Success Factors and Challenges of CIOs

To allow CIOs to serve effectively in the key leadership role envisioned by the Congress, federal agencies should use the full potential of CIOs as information and technology management leaders and active participants in the development of the agency's strategic plans and policies. The CIOs, in turn, must meet the challenges of building credible organizations and developing and organizing information and technology management capabilities to meet mission needs.

In February 2001, we issued guidance on the effective use of CIOs, which describes the following three factors as key contributors to CIO success:

- Supportive 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.
- Effective CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. Placement of the position at an executive management level in the organization is important, but in addition, effective CIOs earn credibility and produce results by establishing effective working relationships with business unit heads.
- Successful CIOs structure their organizations in ways that reflect a clear understanding of

business and mission needs. Along with knowledge of 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 agency needs.

The CIO study that we reported on in July 2004 also provides information on the major challenges that federal CIOs face in fulfilling their duties. In particular, CIOs view IT governance processes, funding, and human capital as critical to their success, as indicated by two challenges that were cited by over 80 percent of the CIOs: implementing effective information technology management and obtaining sufficient and relevant resources.

- Effective IT management.

Leading organizations execute their information technology management responsibilities reliably and efficiently. A little over 80 percent of the CIOs reported that they faced one or more challenges related to implementing effective IT management practices at their agencies. This is not surprising given that, as we have previously reported, the government has not always successfully executed the IT management areas that were most frequently cited as challenges by the CIOs?information security, enterprise architecture, investment management, and e-gov.

- Sufficient and relevant resources.

One key element in ensuring an agency's information and technology success is having adequate resources. Virtually all agency CIOs cited resources, both in dollars and staff, as major challenges. The funding issues cited generally concerned the development and implementation of agency IT budgets and whether certain IT projects, programs, or operations were being adequately funded.

We have previously reported that the way agency initiatives are originated can create funding challenges that are not found in the private sector. For example, certain information systems may be mandated or legislated, so the agency does not have the flexibility to decide whether to pursue them. Additionally, there is a great deal of uncertainty about the funding levels that may be available from year to year.

The government also faces long-standing and widely recognized challenges in maintaining a high-quality IT workforce. In 1994 and 2001, we reported on the importance that leading organizations placed on making sure they had the right mix of skills in their IT workforce. About 70 percent of the agency CIOs reported on a number of substantial IT human capital challenges, including, in some cases, the need for additional staff. Other challenges included recruiting, retention, training and development, and succession planning.

In addition, two other commonly cited challenges were communicating and collaborating (both internally and externally) and managing change.

- Communicating and collaborating.

Our prior work has shown the importance of communication and collaboration, both within an agency and with its external partners. For example, one of the critical success factors we identified in our guide focuses on the CIO's ability to establish his or her organization as a central player in the enterprise. Ten agency CIOs reported that communication and collaboration were challenges. Examples of internal communication and collaboration challenges included (1) cultivating, nurturing, and maintaining partnerships and alliances while producing results in the best interest of the enterprise and (2) establishing supporting governance structures that ensure two-way communication with the agency head and effective communication with the business part of the organization and component entities. Other CIOs cited activities associated with communicating and collaborating with outside entities as challenges, including sharing information with partners and influencing the Congress and OMB.

- Managing change.

Top leadership involvement and clear lines of accountability for making management improvements are critical to overcoming an organization's natural resistance to change, marshaling the resources needed to improve management, and building and maintaining organizationwide commitment to new ways of doing business. Some CIOs reported challenges associated with implementing both changes originating from their own initiative and changes from outside forces. Implementing major IT changes can involve not only technical risks but also nontechnical risks, such as those associated with people and the organization's culture. Six CIOs cited dealing with the government's culture and bureaucracy as challenges to implementing change. Former agency IT executives also cited the need for cultural changes as a major challenge facing CIOs. Accordingly, in order to effectively implement change, it is important that CIOs build understanding, commitment, and support among those who will be affected by the change.

Effectively tackling these reported challenges can improve the likelihood of a CIO's success. Until these challenges are overcome, federal agencies are unlikely to optimize their use of information and technology, which can affect an organization's ability to effectively and efficiently implement its programs and missions.

The CIO Position in the Private Sector Has Similarities to the Federal CIO Position

In September 2005, we reported the results of our study of CIOs at leading private-sector organizations, in which we described the CIOs' responsibilities and major challenges, as well as private-sector approaches to information and technology governance.

The set of responsibilities assigned to CIOs in the private sector were similar to those in the federal sector. In most areas, there was little difference between the private and federal sectors in the percentage of CIOs who had or shared a particular responsibility. In 4 of the 12 areas ? enterprise architecture, strategic planning, information collection, and information dissemination and disclosure?the difference between the private- and federal-sector CIOs was greater; in each case, fewer CIOs in the private sector had these responsibilities. In all, the six functions least likely to be the CIO's responsibility in the federal sector were equivalent to the five functions least likely to be his or her responsibility in the private sector. Some of the federal CIOs' functions, such as information collection and statistical policy, did not map directly to the management areas in several of the private-sector organizations we contacted.

Figure 1 compares federal and private-sector CIO responsibilities for the 12 areas, showing the percentage of CIOs who had or shared responsibility for each area.

Figure 1: Comparison of the Extent to Which Private-Sector and Federal CIOs Are Responsible for Management Areas

Among the private-sector CIOs, it was common to share responsibility with either business units or corporate functional areas; these sharing relationships accounted for almost a third of all responses. Among federal CIOs, the sharing of responsibility was not described in as many areas.

Challenges Identified by Private-Sector CIOs

Approximately half of all the private-sector CIOs described four major challenges:

- Aligning IT with business goals was cited by 11 of the CIOs. This challenge requires the CIOs to develop IT plans to support their companies' business objectives. In many cases this entails cross-organization coordination and collaboration.

- Implementing new enterprise technologies (e.g., radio frequency identification, enterprise resource planning systems, and customer relationship management systems) was cited by 8 of the CIOs. This challenge requires the broad coordination of business and corporate units.
- Controlling IT costs and increasing efficiencies was cited by 9 of the CIOs. Several CIOs explained that by controlling costs and providing the same or better service at lower cost, they are able to contribute to their companies' bottom lines. A few CIOs also said that they generate resources for new investments out of the resources freed up by cost savings.
- Ensuring data security and integrity was cited by 9 of the CIOs. Closely associated with this challenge was ensuring the privacy of data, which was raised by 6 CIOs.

Additional management challenges commonly raised by the private-sector CIOs included

- developing IT leadership and skills (7),
- managing vendors, including outsourcing (7),
- improving internal customer satisfaction (5).

Additional technical challenges commonly raised by the private-sector CIOs included

- implementing customer service/customer relationship management (CRM) systems (7),
- identifying opportunities to leverage new technology (6),
- integrating and enhancing systems and processes (5), and
- rationalizing IT architecture (5).

The challenges mentioned by the private-sector CIOs overlapped with those mentioned by federal CIOs in our previous study. Improving various IT management processes was mentioned by several private-sector CIOs (e.g., IT investment decision making) as well as by federal CIOs, as was developing IT leadership and skills. In technology-related areas, both private-sector and federal CIOs mentioned working with enterprise architectures and ensuring the security of systems as challenges.

Although the challenges mentioned by private-sector CIOs resembled those mentioned by federal CIOs, there were a few differences. Private-sector CIOs mentioned challenges related to increasing IT's contribution to the bottom line?such as controlling costs, increasing efficiencies, and using technology to improve business processes?while federal CIOs tended to mention overcoming organizational barriers and obtaining sufficient resources.

IT Governance in the Private Sector

When asked to describe how the governance of information management and technology is carried out in their companies, 16 of the 20 private-sector companies told us that they had an executive committee with the authority and responsibility for governing major IT investments.

As part of the governance of IT assets in their companies, nine of the CIOs said that they shared responsibility for IT investment management and that their involvement ranged from providing strong leadership to reviewing plans to ensure that they complied with corporate standards.

Many of the private-sector CIOs were actively working to increase coordination among business units to enhance their governance process. Seven of the CIOs described efforts under way to implement enterprisewide financial and supply chain systems, which will move the companies to common business processes. Six CIOs also described using cross-organizational teams (sometimes called centers of excellence), which drive these broad collaborative efforts and others, such as the establishment of standards and common practices.

With regard to the governance of the development of new systems, many of the private-sector CIOs described a process in which they collaborated closely with business units and corporate functional units in planning and developing systems to meet specific needs. The extent of the CIOs' involvement ranged from providing strong leadership and carrying out most activities to reviewing the other components' plans to ensure that they complied with corporate standards.

With regard to sharing authority for decisions on the management of IT assets, several CIOs spoke of balancing between centralization and decentralization of authority and described their efforts to move between the two extremes to find the right balance. The appropriate balance often depended on other events occurring in the companies, such as major strategic realignments or acquisitions. For example, one CIO described his current evolution from a relatively decentralized structure?an artifact of a major effort to enable growth in the corporation?to a more centralized structure in order to reduce costs and drive profits.

Roles and Responsibilities of the CIO Position at VA Have Evolved over Time

Since enactment of the Clinger-Cohen Act in 1996, the roles and responsibilities of VA's Chief Information Officer have evolved. From lacking a CIO entirely, the department has taken steps to address the challenges posed by its multiple widespread components and its decentralized information technology and services.

In June 1998, VA assigned CIO responsibility to a top manager. However, we reported in July 1998 that the person holding the CIO position at VA had multiple additional major responsibilities, as this person also served as Assistant Secretary for Management, Chief Financial Officer, and Deputy Assistant Secretary for Budget. According to the act, the CIO's primary responsibility should be information and technology management. Noting that VA's structure was decentralized, its IT budget was large, and its CIO faced serious information and technology management issues, we recommended that the Secretary appoint a CIO with full-time responsibilities for IRM. Concurring with the recommendation, VA established the position of Assistant Secretary for Information and Technology to serve as its CIO.

As of May 2000, however, the position of Assistant Secretary for Information and Technology was vacant, and as we reported at the time, it had been unfilled since its creation in 1998. The Secretary then created and filled the position of Principal Deputy Assistant Secretary for Information and Technology, designating that person as VA's acting CIO until an Assistant Secretary could be appointed. The Secretary also realigned IRM functions within VA under this position, which reported directly to the Secretary.

As we reported, the Principal Deputy Assistant Secretary was involved in IT planning issues across the department. In addition to advising the Secretary on IT issues, he served as chair of the department's CIO Council and as a member of the department's Capital Investment Board, and he worked with the CIOs in VBA and VHA (at the time, NCA had no CIO). According to this official, one of his priorities was to ensure that IT activities in VBA and VHA were in concert with VA's departmentwide efforts.

In August 2001, VA filled the CIO position. In March 2002, we testified that this hiring was one of the important strides that the Secretary of Veterans Affairs had made to improve the department's IT leadership and management, along with making a commitment to reform the department's use of IT.

On June 29, 2003, the CIO retired after a tenure of almost 2 years (about the median length of tenure for federal CIOs, as discussed above); the current CIO was confirmed in January 2004.

Figure 1 is a time line showing the history of the CIO position at VA since the passage of the Clinger-Cohen Act.

Figure 1: Time Line of CIO Tenure at VA

August 1996: CIO position established by Clinger-Cohen Act July 1998: CIO responsibilities assigned to VA executive June 2000: Deputy assistant secretary position established; acting CIO in position June 29, 2003:
CIO retired; deputy
acts as CIO
⇣ ⇣ ⇣ August 2001: CIO confirmed ⇣ January 2004: CIO confirmed

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005

Vacant
CIO with multiple responsibilities
Acting
Permanent dedicated position

Source: GAO.

VA Proposed to Realign its IT Organization in Response to IT Management Challenges

Our prior work highlighted some of the challenges that the CIO faced as a result of the way the department was organized to carry out its IT mission. Among these challenges was that information systems and services were highly decentralized, and the VA administrations and staff offices controlled a majority of the department's IT budget. For example, in VA's information technology budget for fiscal year 2002 of approximately $1.25 billion, VHA controlled about $1.02 billion (over 80 percent), whereas the department level controlled about $60.2 million (less than 5 percent).

In addition, we 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, we testified that it was crucial for the departmental CIO to ensure that well-established and integrated processes for leading, managing, and controlling investments are commonplace and followed throughout the department. This is consistent with the finding in our CIO review that implementation of IT management practices was a challenge; over half of federal CIOs identified IT investment management specifically.

Recognizing weaknesses in accountability for the department's IT resources and the need to reorganize IT management and financing, the Secretary announced a realignment of the department's IT operations in a memorandum dated August 2002. According to the memorandum, the realignment would centralize IT functions, programs, workforce personnel, and funding into the office of the department-level CIO. In particular, several significant changes were described:

- The CIOs in each of the three administrations?VHA, VBA, and NCA?were to be designated deputy CIOs and were to report directly to the department-level CIO. Previously, these officials served as component-level CIOs who reported only to their respective administrations' under secretaries.

- All administration-level cyber security functions were to be consolidated under the department's cyber security office, and all monies earmarked by VA for these functions were to be placed under the authority of the cyber security officer. Information security officers previously assigned to VHA's 21 veterans integrated service networks would 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 would assume executive authority over VA's IT funding.

In September 2002, we testified that in pursuing these reforms, the Secretary demonstrated the significance of establishing an effective management structure for building credibility in the way IT is used, and took a significant step toward achieving a 'One VA' vision. The Secretary's initiative was also a bold and innovative step by the department?one that has been undertaken by few other federal agencies. For example, of 17 agencies contacted in 2002, 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.

We also noted that the CIO's success in managing IT operations under the realignment would hinge on effective collaboration with business counterparts to guide IT solutions that meet mission needs, and we pointed out the importance of the three key contributors to CIO success described in our 2001 guidance (discussed earlier).

Although we have not reviewed the current status of this proposed realignment or VA's current organizational structure, it remains our view that the proposed realignment held promise for building a more solid foundation for investing in and improving the department's accountability over IT resources. Specifically, under the realignment the CIO would assume budget authority over all IT funding, including authority to veto proposals submitted from subdepartment levels. This could have a significant effect on VA's accountability for how components are spending money.

To sum up, the CIO plays a vital role in ensuring that VA's funds are well spent and in managing information technology to serve our nation's veterans. In our view, the realignment of VA's IT organization proposed in 2002 held promise for improving accountability and enabling the department to accomplish its mission. The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively account for and manage its proposed $2.1 billion in planned IT spending.

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

Contacts and Acknowledgements

For information about this testimony, please contact Linda D. Koontz, Director, Information Management Issues, at (202) 512-6240 or at koontzl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Individuals making key contributions to this testimony include Barbara Collier, Lester Diamond, Barbara Oliver, and J. Michael Resser.

(310747)