STATEMENT OF JEFFREY W. SEIFERT
ANALYST IN INFORMATION SCIENCE AND TECHNOLOGY POLICY
CONGRESSIONAL RESEARCH SERVICE

BEFORE

THE COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES
SEPTEMBER 14, 2005
VA IT Infrastructure Reorganization and the Role of the CIO

Mr. Chairman, and members of the Committee, thank you for the invitation to appear before you today to offer testimony on the background and role of chief information officers (CIOs) in the federal government. While the primary focus of today's hearing is on responsibilities and authority entrusted to the Office of the Chief Information Officer at the Department of Veterans Affairs (VA), my comments today will be restricted to the performance and challenges of federal CIOs more generally. As you are aware, the Congressional Research Service does not take a position on issues or legislation. Consequently, I will confine my remarks to the historical and organizational aspects of today's topic.

The Importance of Federal IT Management

The federal government spends more than $60 billion annually on information technology (IT) goods and services. As information technology becomes increasingly integrated into nearly all government processes, efforts to improve federal IT management have become more important. These include initiatives to develop a federal enterprise architecture, improve information security, and identify opportunities to facilitate information sharing. Consolidating authority over IT resources and clarifying who is accountable for specific functions is part of this process. However, the broad range of activities and fluid nature of federal information technology initiatives suggest that the level of consolidated control will likely depend on the size and nature of the responsibilities of each department.

Federal CIOs are on the front lines in implementing a wide range of e-government and homeland security initiatives. In the case of e-government a central area of concern is developing a comprehensive but flexible strategy to coordinate the disparate e-government initiatives across the federal government. As the initial round of e-government projects continue to become fully operational, OMB has stated it plans to focus attention on initiatives that consolidate information technology systems in six functional Lines of Business (LoB). These include financial management, human resource management, grants management, case management, federal health architecture, and information security. These initiatives were chosen, in part, because they represent core business functions common to many departments and agencies, and/or have the potential to reap significant efficiency and efficacy gains. These LoB initiatives are anticipated to create $5 billion in savings over 10 years.

In considering the VA, it may be instructive to took at another department. In the case of homeland security, one of the biggest challenges facing the Department of Homeland Security (DHS) is the ongoing effort to consolidate the computer and communications systems of the 22 agencies that comprise the Department. In many respects, DHS functions as a virtual department, connecting new and existing agencies into a network that capitalizes on their knowledge assets to facilitate information sharing and enhanced communication. Organizationally, this involves breaking down the "stovepipes" that have previously separated the agencies and developing an encompassing organizational culture that promotes cooperation and information sharing. Technologically, this involves integrating existing systems and infrastructures while simultaneously infusing new technologies as they are become available. A critical variable that will contribute to the success or failure of these objectives is the development and implementation of an enterprise architecture for the Department. An enterprise architecture serves as a blueprint of the business operations of an organization, and the technologies needed to carry out these functions. It is designed to be comprehensive, flexible, and scalable, to account for future growth needs. As the Department moves forward with its enterprise architecture plans, it will encounter several issues, including making choices between competing systems and reallocating resources and staff accordingly.

Origins of Establishment of Chief Information Officer (CIO) Position

During the mid-1990s, Congress considered several bills focusing on governmental reform and improved management of public resources. The option of establishing a single federal CIO was one of several proposals to address these problems. The success of CIOs in the private sector is often cited as an example for government to follow. However, the interest in establishing CIOs in the federal government was generated by the experience of local and state governments. At the time, forty states had some form of a CIO operating in a policy capacity, as did several major cities. For many, their experience demonstrated that there was a need for someone to articulate a "vision" of information resources that helped coordinate agency activities and goals rather than reinforce the artificial "stovepipes" that separated them. The idea of a federal CIO was ultimately dropped in favor of establishing a CIO in each of the major executive branch agencies, which was included as one of the provisions in the Information Technology Management Reform Act (ITMRA), which was enacted into law as Section E of the National Defense Authorization Act for Fiscal Year 1996, (P.L. 104-106). Another provision of P.L. 104-106 was the Federal Acquisition Reform Act (FARA) (Section D). FARA and ITMRA were collectively renamed the Clinger-Cohen Act of 1996 in the fiscal year 1997 Omnibus Consolidated Appropriations Act, (P.L. 104-208).

The statutory responsibilities of federal CIOs are delineated in Section 5125(b) of the Clinger-Cohen Act:

> (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with

> chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency;
>
> (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and
>
> (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

In addition, as the individuals primarily responsible for IT capital planning and investment control in their respective departments, federal CIOs are required to report to their department heads. Besides the Clinger-Cohen Act, other laws that affect or modify CIOs' responsibilities include the Paperwork Reduction Act of 1995, the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), the Federal Records Act, the Freedom of Information Act, and the Privacy Act of 1974. Although these responsibilities suggest that federal CIOs are the primary officials in charge of planning, acquiring, and maintaining IT resources in their respective departments and agencies, the Clinger-Cohen Act does not *explicitly* identify federal CIOs as having any budgetary control or authority over IT resources.

Chief Information Officers Council

Following the passage of the Clinger-Cohen Act, President Clinton established the Chief Information Officers Council by Executive Order 13011, *Federal Information Technology*, on July 16, 1996. The CIO Council was later codified into statute with the passage of the E-Government Act of 2002 (P.L. 107-347) in December 2002. Section 101 of the E-Government Act adds chapter 36 "Management and Promotion of Electronic Services" to Title 44 of the United States Code. Among other provisions, this chapter delineates the membership and responsibilities of the CIO Council, which is described as the "principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources."[1] The membership of the CIO Council includes, the CIOs of the major executive branch departments and agencies; the CIOs of the Central Intelligence Agency (CIA), Army, Navy, and Air Force; the Administrator of the Office of Electronic Government; the Administrator of the Office of Information and Regulatory Affairs (OIRA); the Deputy Director for Management of the Office of Management and Budget (OMB), who serves as the chairperson of the CIO Council; and any other officer or employee of the United States designated by the chairperson. The Administrator of the Office of E-Government leads the activities of the CIO Council on behalf of the chairperson and the Vice Chair is elected from the membership. The CIO Council meets monthly and currently has three committees to address specific information technology management concerns such as enterprise architecture development, IT workforce issues, and information technology best practices. The committees work to help facilitate the growth of government standards, share best practices, and help agencies work to be in compliance with reform legislation such as the Government Performance and Results Act (GPRA).

[1] 3603 (d).

The statutory responsibilities of the CIO Council are delineated in Section 3603 of Chapter 36 U.S.C., as stated in the E-Government Act:

> (1) Develop recommendations for the Director on Government information resources management policies and requirements.
>
> (2) Share experiences, ideas, best practices, and innovative approaches related to information resources management.
>
> (3) Assist the Administrator in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.
>
> (4) Promote the development and use of common performance measures for agency information resources management under this chapter and title II of the E-Government Act of 2002.
>
> (5) Work as appropriate with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40, and maximize the use of commercial standards as appropriate, including the following:
>
> > (A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.
> >
> > (B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.
> >
> > (C) Standards and guidelines for Federal Government computer system efficiency and security.
>
> (6) Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management.
>
> (7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

Evolving Role of Federal CIOs

As IT projects have become more integrated into the function of a department or agency, the role of CIOs has evolved as well. While CIOs were once commonly thought of as “technocrats,” they are now being called upon not only for their technological expertise, but also to provide strategic leadership in the areas of policy, budget, and contract oversight. Federal CIOs serve the role of change agents for business modernization and transformation. They must possess strong management, leadership, and communication skills. The CIO’s relationship with top-level department decisionmakers can also be critical to successfully implementing IT and e-government initiatives. This suggests that, in selecting a department-level CIO, one needs to select individuals who have a deep contextual understanding of the mission and functions of an organization, but who also bring a wide range of experiences and perspectives to the position.

Inherent to the nature of their responsibilities, CIOs need to look at their departments horizontally, across a department, rather than vertically, such as at a single program or function. Likewise, there is a need to be able to exercise control over resources horizontally, across a department, in part to break down so-called “stovepipes” and “islands of automation” that can be created when resources and programs are developed vertically. However, this perspective can frequently put the CIO at odds with his/her counterparts, such as program managers, whose responsibilities may foster a more vertical view of the department and its assets. For example, whereas CIOs may want to move the department to adopt a standardized software platform for desktop computers in order to facilitate interoperability and lower costs, program managers may oppose this approach on the basis that it reduces their decisionmaking authority to procure and develop assets used in the delivery of services. This clash of perspectives is frequently one of the root causes of the most significant challenges federal CIOs face.

Challenges Facing CIOs

Since the creation of the department-level chief information officer position, a number of obstacles have been attributed to undermining the CIOs’ abilities to carry out their responsibilities. For example, at a July 2004 hearing of the House Committee on Government Reform’s Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, in his opening statement, the Subcommittee Chairman highlighted some of the more pressing issues related to federal CIOs. These included the disparity between the average tenure of an agency CIO (23 months) and the amount of time it takes to effect change and shepherd large projects (3-5 years); CIOs’ lack of control over all IT investment in their agencies; the growing range of CIO responsibilities; and the reporting relationships between CIOs and senior management as well as subordinates.[2]

In its 2004 annual survey of federal chief information officers, the Association for Federal Information Resource Managers (AFFIRM) asked respondents to rank order the most important

[2] Opening statement of the Hon. Adam Putnam: House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, *Where’s the CIO? The Role, Responsibility and Challenge for Federal Chief Information Officers in IT Investment Oversight and Management,* 108th Cong., 2nd sess. (Washington: GPO, 2004), p. 4.

challenges they faced. The top ten reported challenges, starting with the most important challenge cited, include:

- *Aligning IT and organizational mission goals*
- Using IT to improve service to customers/stakeholders/citizens
- *Obtaining adequate funding for IT programs and projects*
- *Formulating or implementing an enterprise architecture*
- Hiring and retaining skilled professionals
- Managing or replacing legacy systems
- *Developing agency-wide IT accountability*
- *Unifying "islands of automation" within lines of business (across agencies)*
- *Implementing and controlling IT capital planning and investment management across the agency*
- Simplifying business processes to maximize the benefit of technology[3]

Six of the top ten reported challenges (shown in italics above) are directly related to the CIO's ability to exercise department-wide authority over IT personnel, assets, and resources. As e-government and homeland security initiatives become more sophisticated and move beyond their demonstration project phases, they begin to assume a department-wide, or even government-wide character. Consequently, the CIO's authority over relevant resources can be crucial to the longer term implementation and success of these initiatives.

Although the specific issues may differ slightly from year to year, there is general agreement that the biggest challenges facing federal CIOs are not technical, but instead, organizational. Decentralized organizations can pose especially trying challenges for CIOs, whose primary role includes coordinating resources and personnel from a horizontal, centralized perspective in an effort to effect transformation of the organization. A factor frequently cited by experts on federal IT management that affects the CIO's performance is whether or not he/she has a seat at the management table. Although the Clinger-Cohen Act requires that department-level CIOs report to the Secretaries of their respective departments, in practice this is not always the case. Instead, they may be reporting to officials one, two, or possibly three levels below the department secretary. While there is some debate regarding whether there is no substitute for reporting directly to the department secretary, or if reporting to an alternative senior official, such as a chief management officer is sufficient, there is clear agreement that being able to influence top-level decisionmaking can be critical to the CIO's ability to carry out his/her responsibilities. Access to, or direct participation in, decisions regarding funding issues and the allocation of resources can have a significant impact on agency IT budgets and whether various initiatives and programs are adequately funded. However, simply having a seat at the management table may not be sufficient if other parts of the department can act autonomously in areas that either undermine or mitigate attempts by the CIO to develop enterprise-wide standards. To that end, there appears to be a growing interest on the part of some departments and agencies to expand their CIOs' authority and control over all of their respective department's IT budgetary and

[3] AFFIRM, *The Federal Chief Information Officer: Ninth Annual Top Ten Challenges Survey*, (Washington: December 2004), p. 11.

information resources, and in some cases, IT-related personnel as well, rather than leaving some control in the hands of project managers and other department officials.

Selected Recent Attempts by Federal Departments and Agencies to Address Challenges

The Clinger-Cohen Act divides responsibility for federal IT management among three primary entities; OMB, department heads, and department CIOs. If the performance of any one of these entities is reduced, or diminished, then federal IT management as a whole can suffer. As a result of organizational resistance to transformational change, it is possible that CIOs may need additional tools and authority to carry out their responsibilities as the federal government continues to move into the 21st century. To that end, there appears to be a growing awareness of the importance of budgetary control to IT management, and some departments have begun addressing this issue.

For example, earlier this year, following the high-profile failure of its Virtual Case File (VCF) initiative, designed to provide Federal Bureau of Investigation (FBI) agents with a computerized case management system at their desktops, the FBI announced it was implementing a new strategic approach to information technology. Specifically, the strategy includes centralizing management of FBI IT under the FBI's Office of the Chief Information Officer (OCIO), creating several IT governance boards, implementing an enterprise architecture and an IT investment strategy, and granting the OCIO "budgetary authority over all FBI IT funds."[4]

In an effort to both strengthen federal CIOs' budgetary authority and enhance congressional oversight, some observers have suggested consolidating a department's entire IT spending under a single budgetary line item. However, the possibility of attempting to define a department's entire IT spending under a single budgetary line item may be complicated by the object classes used to identify particular expenditures, because each object class may include a variety of similar, but unrelated, expenditures.[5] Consequently, some attempts to address the issue of CIO budgetary control do not necessarily extend to a department's entire IT investment, but only to specific initiatives. For example, in the President's FY2006 budget proposal, the Department of Justice (DOJ) is to receive funding to facilitate and improve information sharing. These monies are to be placed in a centralized fund, the Justice Information Sharing Technology (JIST) account, which in turn is to be controlled by the DOJ CIO. The rationale provided for centralizing control over these monies is to:

[4] Federal Bureau of Investigation, FBI Information Technology Fact Sheet, June 8, 2005, available at: [http://www.fbi.gov/pressrel/pressrel05/factsheet.htm].

[5] IT-related expenditures can be classified into at least six object classes. These include 23.3 Communications, Utilities, and Miscellaneous Charges; 25.1Advisory and Assistance Services; 25.2 Other Services; 25.7 Operation and Maintenance of Equipment; 26.0 Supplies and Materials; and 31.0 Equipment. A more complete explanation of what is specifically included and excluded from each of those object classes is explained in Section 83 of OMB Circular No. A-11, 2004, available online at: [http://www.whitehouse.gov/omb/circulars/a11/current_year/s83.pdf]. Revised guidance for reporting information technology investments for the FY 2006 budget formulation process are explained in Section 53 of OMB Circular No. A-11, 2004, available online at: [http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf].

> ensure that investments in information sharing technology are well-planned and aligned with the Department's overall information technology (IT) strategy and enterprise architecture, and that all DOJ components are able to operate in a technologically unified environment, particularly with respect to preventing terrorist attacks on the United States.[6]

Efforts to consolidate IT investment management decisions can also be complicated by a lack of comprehensive accounting of a department's IT resources and responsibilities at the outset. For example, in its March 2005 report regarding the OCIO's budget, the Inspector General at the Department of Transportation (DOT) found that the consolidation of department-wide IT responsibilities, including management of its telephone switching network and provision of network services to the department's operating administrations (OAs), begun in FY2003, was not accompanied by a comparable level of budgetary and contract services oversight. Among the problems specifically identified in consolidating OCIO control over systems originally maintained by the eleven individual OAs, was an incommensurate transfer of project management and budget authority and duplicative funding requests made by the OCIO and the OAs. In response, the DOT IG made nine recommendations for the DOT CIO to follow, including "analyzing performance gaps among duplicate systems in the 11 common businesses" in order to "recommend to the Investment Review Board how consolidating these systems should be funded and managed," and to improve coordination between the OCIO and the OAs to avoid duplicate funding requests for performing similar tasks.[7]

Conclusion

In closing, information technology management has been a long-standing challenge for many federal departments and agencies. The general problems facing the Department of Veterans Affairs are not unlike those facing CIOs in other executive branch departments and agencies. However, the challenges of harmonizing the acquisition, development, and maintenance of information resources across the department, including its three major subcomponents, the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration (NCA), are considerable. By enhancing the authority of the CIO, the Department of Veterans Affairs may be able to better address some of its information technology management challenges in the future. Thank you for your attention. I welcome any questions.

[6] U.S. Office of Management and Budget, *Budget of the U.S. Government, Fiscal Year 2006: Appendix*, (Washington: GPO, 2005), p. 672.

[7] Department of Transportation, Office of the Secretary, Office of the Inspector General, *Office of the Chief Information Officer's Budget*, Report FI-2005-055, March 31, 2005, pp. 12-13.