United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

INFORMATION AND TECHNOLOGY MANAGEMENT

Responsibilities, Reporting Relationships, Tenure, and Challenges of Agency Chief Information Officers

Statement of David A. Powner,
Director, Information Technology
 Management Issues

GAO

Accountability * Integrity * Reliability

GAO-04-957T

July 21, 2004

INFORMATION AND TECHNOLOGY MANAGEMENT

Responsibilities, Reporting Relationships, Tenure, and Challenges of Agency Chief Information Officers

Why GAO Did This Study

Federal agencies rely extensively on information technology (IT) to effectively implement major government programs. To help agencies manage their substantial IT investments, the Congress has established a statutory framework of requirements, roles, and responsibilities relating to IT management.
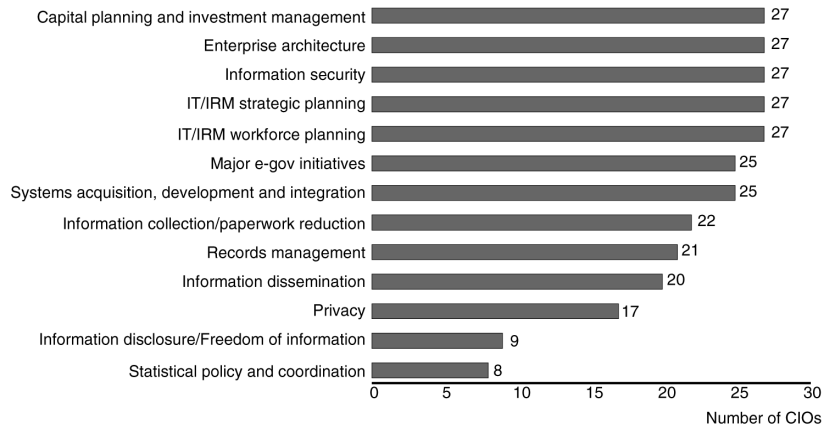
GAO was asked to summarize its report, being issued today, on federal chief information officers' (CIO) responsibilities, reporting relationships, and tenure and on the challenges that CIOs face (*Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823, July 21, 2004) and to offer suggestions for actions that both the Congress and the agencies can take in response to these findings.

www.gao.gov/cgi-bin/getrpt?GAO-04-957T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David A. Powner at 202-512-9286 or pownerd@gao.gov.

What GAO Found

In looking at 27 agencies, GAO found that CIOs generally were responsible for most of the 13 areas that had been identified as either required by statute or critical to effective information and technology management (see figure below) and that about 70 percent reported directly to their agency heads. Among current CIOs and former agency IT executives, views were mixed on whether it was important for the CIO to have responsibility for each of the 13 areas and a direct reporting relationship with the agency head. In addition, current CIOs come from a wide variety of professional and educational backgrounds and, since the enactment of the legislation establishing this position, the permanent CIOs who had completed their time in office had a median tenure of about 2 years. Their average time in office, however, was less than the 3 to 5 years that both current CIOs and former agency IT executives most commonly cited as the amount of time needed for a CIO to be effective. Too short of a tenure can reduce a CIOs' effectiveness and ability to address major challenges, including implementing effective IT management and obtaining sufficient and relevant resources.

Both the Congress and the federal agencies can take various actions to address GAO's findings. First, as the Congress holds hearings on and introduces legislation related to information and technology management, there may be an opportunity to consider the results of this review and whether the existing statutory framework offers the most effective structure for CIOs' responsibilities and reporting relationships. Second, agencies can use the guidance GAO has issued over the past few years to address, for example, agencies' IT management and human capital challenges. Finally, agencies can also employ such mechanisms as human capital flexibilities to help reduce CIO turnover or to mitigate its effect.

Number of CIOs with Responsibility for Information Technology Management Areas

Management Area	Number of CIOs
Capital planning and investment management	27
Enterprise architecture	27
Information security	27
IT/IRM strategic planning	27
IT/IRM workforce planning	27
Major e-gov initiatives	25
Systems acquisition, development and integration	25
Information collection/paperwork reduction	22
Records management	21
Information dissemination	20
Privacy	17
Information disclosure/Freedom of information	9
Statistical policy and coordination	8

Number of CIOs

Source: Agency CIOs.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing on federal agency chief information officers (CIO). Our work and the work of others have shown that the federal government has had long-standing information and technology management problems. Various laws have been enacted to improve the government's performance in this area. For example, the Clinger-Cohen Act of 1996 requires agency heads to designate CIOs to lead reforms to help control system development risks, better manage technology spending, and achieve real, measurable improvements in agency performance through better management of information resources.

At your request, I will summarize our report[1] being issued today that focuses on the status of federal CIOs, including their responsibilities and reporting relationships, professional backgrounds and tenure, and what they viewed as their major challenges. In addition, I will discuss what can be done to address our findings. In performing our work at 27 major federal departments and agencies (23 entities identified in 31 United States Code 901,[2] the Department of Homeland Security, and the 3 military services),[3] we initially collected information using a data collection instrument and subsequently interviewed each of the CIOs who were in place at the time of our review. We also conducted two panel discussions with former agency information technology (IT) executives, including former CIOs, that addressed their experiences and challenges, and we held a series of discussions with our Executive Council on Information Management and Technology, which is composed of noted IT experts from the public and private sectors and from academia. The work on which this

---

[1]U.S. General Accounting Office, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

[2]This section of the U. S. C. requires 24 departments and agencies to establish chief financial officers. We did not include the Federal Emergency Management Agency in our review, even though it is one of the 24 departments and agencies, because this agency has been transferred to the Department of Homeland Security.

[3]The 27 agencies covered by our report are the Departments of Agriculture, the Air Force, the Army, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, the Navy, State, Transportation, the Treasury, and Veterans Affairs; and the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

testimony is based was performed from November 2003 through May 2004 in accordance with generally accepted government auditing standards.

Results in Brief

Generally, CIOs were responsible for most of the 13 areas we identified as either required by statute or critical to effective information and technology management, and about 70 percent of the CIOs reported directly to their agency heads. However, two of the information and technology management areas—information disclosure and statistics—were the responsibility of fewer than half of the CIOs. While this alternative assignment of responsibility is not consistent with the statutes, the CIOs generally believed that not being responsible for certain information and technology management areas did not present a problem, in large part because other organizational units were assigned these duties. Views were mixed among current CIOs and former agency IT executives on whether a direct reporting relationship was crucial to the success of the CIO. In addition, current CIOs come from a wide variety of professional and educational backgrounds, and since the enactment of the Clinger-Cohen Act, the permanent CIOs who had completed their time in office had a median tenure of about 2 years. Agency CIOs' average time in office, however, was less than the 3 to 5 years that was most commonly cited by both current CIOs and former agency IT executives as the amount of time needed for a CIO to be effective. This difference in tenure can negatively impact CIOs' effectiveness and their ability to address the major challenges they cited. These challenges include implementing effective IT management and obtaining sufficient and relevant resources.

The Congress and federal agencies can take various actions to address our findings. First, as the Congress holds hearings on and introduces legislation related to information and technology management, there may be an opportunity to consider the results of this review and whether the existing statutory framework offers the most effective structure for CIOs' responsibilities and reporting (i.e., to the agency head). Second, agencies can use the guidance we have issued over the past few years to address, for example, their IT management and human capital challenges. In addition, various mechanisms, such as human capital flexibilities, are available for agencies to use to help reduce CIO turnover or to mitigate its effect.

Background

Despite a substantial investment in IT, the federal government's management of information resources has produced mixed results.

Although agencies have taken constructive steps to implement modern strategies, systems, and management policies and practices, we continue to find that agencies face significant challenges.[4] The CIO position was established by the Congress to serve as the focal point for information and technology management issues within an agency, and CIOs can address these challenges with strong and committed leadership.

The Congress has assigned a number of responsibilities to the CIOs of federal agencies. (See app. I for a summary of the legislative evolution of agency CIO responsibilities.) In addition, we have identified other areas of information and technology management that can contribute significantly to the successful implementation of information systems and processes. Altogether, we identified the following 13 major areas of CIO responsibilities as either statutory requirements or critical to effective information and technology management:[5]

- *IT/IRM strategic planning.* CIOs are responsible for strategic planning for all information and information technology management functions—referred to by the term information resources management (IRM) strategic planning [44 U.S.C. 3506(b)(2)].

- *IT capital planning and investment management.* CIOs are responsible for IT capital planning and investment management [44 U.S.C. 3506(h) and 40 U.S.C. 11312 & 11313].

- *Information security.* CIOs are responsible for ensuring their agencies' compliance with the requirement to protect information and systems [44 U.S.C. 3506(g) and 3544(a)(3)].

- *IT/IRM human capital.* CIOs have responsibilities for helping their agencies meet their IT/IRM workforce needs [44 U.S.C. 3506(b) and 40 U.S.C. 11315(c)].

---

[4]U.S. General Accounting Office, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 1, 2003) and *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-03-95 (Washington, D.C.: January 1, 2003).

[5]Three 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.

- *Information collection/paperwork reduction.* CIOs are responsible for the review of their agencies' information collection proposals to maximize the utility and minimize public paperwork burdens [44 U.S.C. 3506(c)].

- *Information dissemination.* CIOs are responsible for ensuring that their agencies' information dissemination activities meet policy goals such as timely and equitable public access to information [44 U.S.C. 3506(d)].

- *Records management.* CIOs are responsible for ensuring that their agencies implement and enforce records management policies and procedures under the Federal Records Act [44 U.S.C. 3506(f)].

- *Privacy.* CIOs are responsible for their agencies' compliance with the Privacy Act and related laws [44 U.S.C. 3506(g)].

- *Statistical policy and coordination.* CIOs are responsible for their agencies' 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)].

- *Information disclosure.* CIOs are responsible for information access under the Freedom of Information Act [44 U.S.C. 3506(g)].

- *Enterprise architecture.* Federal laws and guidance direct agencies to develop and maintain enterprise architectures as blueprints to define the agency mission and the information and IT needed to perform that mission.

- Systems acquisition, development, and integration. GAO has found that a critical element of successful IT management is effective control of systems acquisition, development, and integration [44 U.S.C. 3506(h)(5) and 40 U.S.C. 11312].

- *E-government initiatives.* Various laws and guidance direct agencies to undertake initiatives to use IT to improve government services to the public and internal operations [44 U.S.C. 3506(h)(3) and the E-Government Act of 2002].

CIOs' Responsibilities, Reporting Relationships, Tenure, and Challenges

The agency CIOs were generally responsible for most of the 13 key areas we identified as either required by statute or among those critical to effective information and technology management, and most of these CIOs reported directly to their agency heads. We found that only 2 of these 13 areas were cited as the responsibility of fewer than half of the CIOs, and 19 of the CIOs reported directly to their agency heads. Their median tenure was about 2 years—less than the 3 to 5 years that CIOs and former senior agency IT executives said were necessary for a CIO to be effective; this gap could be problematic because it could inhibit CIOs' efforts to address major challenges, including IT management and human capital.

Agency CIOs Generally Were Responsible for Most Areas

As figure 1 illustrates, CIOs were responsible for key information and technology management areas. In particular, 5 of the 13 areas were assigned to every agency CIO. These areas were capital planning and investment management, enterprise architecture, information security, IT/IRM strategic planning, and IT workforce planning. However, of the other 8 areas, 2 of them—information disclosure and statistics—were the responsibility of fewer than half of the CIOs. Disclosure is a responsibility that has frequently been assigned to offices such as general counsel and public affairs in the agencies we reviewed, while statistical policy is often the responsibility of separate offices that deal with the agency's data analysis, particularly in agencies that contain Principal Statistical Agencies.[6] Nevertheless, even for those areas of responsibility that were not assigned to them, the CIOs generally reported that they contributed to the successful execution of the agency's responsibility.

---

[6]Principal Statistical Agencies include the Bureau of Economic Analysis (Department of Commerce), Bureau of Justice Statistics (Department of Justice), Bureau of Labor Statistics (Department of Labor), Bureau of Transportation Statistics (Department of Transportation), Economic Research Service (Department of Agriculture), Energy Information Administration (Department of Energy), Environmental Protection Agency, Internal Revenue Service's Statistics of Income Division (Department of the Treasury), National Agricultural Statistics Service (Department of Agriculture), National Center for Education Statistics (Department of Education), National Center for Health Statistics (Department of Health and Human Services), Science Resources Statistics (National Science Foundation), Office of Policy (Social Security Administration), Office of Management and Budget (Executive Office of the President), and the U.S. Census Bureau (Department of Commerce)

Figure 1: Number of CIOs Reporting That They Were Responsible for Each Information and Technology Management Area

Management Area	Number of CIOs
Capital planning and investment management	27
Enterprise architecture	27
Information security	27
IT/IRM strategic planning	27
IT/IRM workforce planning	27
Major e-gov initiatives	25
Systems acquisition, development and integration	25
Information collection/paperwork reduction	22
Records management	21
Information dissemination	20
Privacy	17
Information disclosure/Freedom of information	9
Statistical policy and coordination	8

Number of CIOs (x-axis: 0, 5, 10, 15, 20, 25, 30)

Source: Agency CIOs.

In those cases where the CIOs were not assigned the expected responsibilities, and they expressed an opinion about the situation,[7] more than half of the CIO responses were that the applicable information and technology management areas were appropriately held by some other organizational entity. Moreover, one of the panels of former agency IT executives suggested that not all 13 areas were equally important to CIOs. A few of the former agency IT executives even called some of the areas relating to information management a distraction from the CIO's primary responsibilities. Those sentiments, however, are not consistent with the law, which envisioned that having a single official responsible for the various information and information technology functions would provide integrated management.

Specifically, one purpose of the Paperwork Reduction Act of 1980 (PRA) is to coordinate, integrate, and—to the extent practicable and appropriate—make federal information resources management policies and practices uniform as a means to improve the productivity, efficiency, and effectiveness of government programs by, for example, reducing information collection burdens on the public and improving service

---

[7]Out of a total of 69 possible responses (instances of CIOs without responsibility for one or more of the 13 information and technology management areas), in 42 instances CIOs expressed an opinion on whether they had any concerns with their agency's assignment.

delivery to the public. Moreover, the House committee report accompanying the PRA in 1980 asserted that aligning IRM activities under a single authority should provide for both greater coordination among an agency's information activities and higher visibility for these activities within the agency.[8]

In addition to specifying areas of responsibility for the CIOs of major departments and agencies, the Clinger-Cohen Act calls for certain CIOs to have IRM as their primary duty.[9] All but a few of the agencies complied with this requirement. The other significant duties reported by some CIOs generally related to other administrative or management areas, such as procurement and human capital. We[10] and Members of Congress[11] have previously expressed concern about agency CIOs having responsibilities beyond information and technology management and have questioned whether dividing time between two or more kinds of duties would allow CIOs to deal effectively with their agencies' IT challenges.

CIOs Generally Reported to Their Agency Heads

Federal law—as well as our guide based on CIOs of leading private sector organizations—generally calls for CIOs to report to their agency heads,[12] forging relationships that ensure high visibility and support for far-reaching information management initiatives. Nineteen of the CIOs in our review 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.

---

[8]U.S. House of Representatives, *Paperwork Reduction Act of 1980*, House Report 96-835, (Washington, D.C., Mar. 19, 1980).

[9]The Clinger-Cohen Act requirement that agency CIOs have IRM as their primary duty applies to the major departments and agencies listed in 31 U.S.C. 901(b), which does not include the Department of Homeland Security or the Departments of the Air Force, the Army, and the Navy.

[10]U.S. General Accounting Office, *Chief Information Officers: Ensuring Strong Leadership and an Effective Council*, GAO/T-AIMD-98-22 (Washington, D.C.: Oct. 27, 1997).

[11]U.S. Senate Committee on Governmental Affairs, *Paperwork Reduction Act of 1995*, Senate Report 104-8 (Washington, D.C., Jan. 30, 1995).

[12]The Homeland Security Act of 2002 states that the CIO for the Department of Homeland Security shall report to the Secretary of Homeland Security or to another official as directed by the Secretary. As allowed by the law, the Secretary has directed the CIO to report to the Under Secretary for Management.

The views of current CIOs and former agency IT executives about whether it is important for the CIO to report to the agency head were mixed. For example, of the 8 CIOs who did not report directly to their agency heads, (1) 3 stated it was important or critical, (2) 2 stated it was not important, (3) two stated it was generally important but that the current reporting structure at their agencies worked well, and (4) 1 stated it was very important that a CIO report to at least a deputy secretary. In contrast, 15 of the 19 CIOs who reported to their agency heads stated that this reporting relationship was important.[13] However, 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. Finally, members of our Executive Council on Information Management and Technology told us that what is most critical is for the CIO to report to a top level official. The members of our panels of former agency IT executives also had a variety of views on whether it was important that the CIO report to the agency head.

CIOs Have Diverse Backgrounds and Generally Remained in Office about 2 Years

At the major departments and agencies included in our review, the current CIOs had diverse backgrounds, and since the enactment of the Clinger-Cohen Act, the median tenure of permanent CIOs whose time in office had been completed was about 2 years.[14] Both of these factors can significantly influence whether a CIO is likely to be successful. First, the background of the current 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. Virtually all of them had work experience and/or educational backgrounds in IT or IT-related fields. For example, 12 current agency CIOs had previously served in a CIO or deputy CIO capacity. Moreover, most of the CIOs 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.

Second, the median time in the position for agencies' permanent CIOs was 23 months. For career CIOs, the median was 32 months; the median for political appointees was 19 months. When asked how long a CIO needed to

---

[13]One agency CIO stated that reporting to the CIO was not important, one CIO did not clearly address the question, and we not discussed this issue with two CIOs.

[14]We did not include acting CIOs in this calculation, unless the acting CIO was later put in the permanent position. Further analysis of tenure data is provided in appendix IV.

stay in office to be effective, the most common response of current CIOs and former agency IT executives 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 views of many agency CIOs, who believed that the turnover rate was high and that the political environment, the pay differentials between the public and private sectors, and the challenges that CIOs face contributed to this rate.

Agency CIOs Face Major Challenges

Current CIOs reported that they faced major challenges in fulfilling their duties. In particular, two challenges were cited by over 80 percent of the CIOs: implementing effective information technology management and obtaining sufficient and relevant resources. This indicates that CIOs view IT governance processes, funding, and human capital as critical to their success. Other common challenges they cited were communicating and collaborating internally and externally and managing change. Effectively tackling these reported challenges can improve the likelihood of a CIO's success. The challenges the CIOs identified were as follows:

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.[15]

Sufficient and Relevant Resources. One key element in ensuring an agency's information and technology success is having adequate resources available. 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.

---

[15]See, for example, U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*; GAO-03-121 (Washington, D.C.: Jan. 1, 2003); GAO-04-49; GAO-04-40; and GAO-03-95.

We have previously reported that the way agency initiatives are originated can create funding challenges that are not found in the private sector.[16] 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 the importance that leading organizations placed on making sure they had the right mix of skills in their IT workforce.[17] 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.

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 CIO guide focuses on the CIO's ability to establish his or her organization as a central player in the enterprise.[18] 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 the Office of Management and Budget (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

---

[16]U.S. General Accounting Office, *Chief Information Officers: Implementing Effective CIO Organizations*, GAO/T-AIMD-00-128 (Washington, D.C.: Mar. 24, 2000).

[17]U.S. General Accounting Office, *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1, 1994) and GAO-01-376G.

[18]GAO-01-376G.

resources needed to improve management, and building and maintaining organizationwide commitment to new ways of doing business. Some CIOs reported challenges associated with implementing changes originating both from their own initiative and 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.

Actions Can Be Taken to Improve Agencies' Information and Technology Management

The Congress and agencies can take various actions to assist CIOs in fulfilling their vital roles. With respect to the Congress, hearings such as this, Mr. Chairman, help to raise issues and suggest solutions. Also, the report we are releasing today contains a Matter for Congressional Consideration in which we suggest that, as you hold hearings on and introduce legislation related to information and technology management, you consider whether the existing statutory requirements related to CIO responsibilities and reporting to the agency head reflect the most effective assignment of information and technology management responsibilities and the best reporting relationship. To further assist in your oversight role, as you requested, we are beginning work on the development of a set of CIO best practices, based on the practices of leading organizations in the private sector, to complement the report we are releasing today.

Agencies, too, can take action to improve their information and technology management. First, to address concerns about the high CIO turnover rate, agencies may be able to use human capital flexibilities—which represent the policies and practices that an agency has the authority to implement in managing its workforce—to help retain its CIOs. For example, our model on strategic human capital management notes that recruiting bonuses, retention allowances, and skill-based pay can attract and retain employees who possess the critical skills the agency needs to accomplish its mission.[19] We have also issued several reports that discuss these issues in more depth and provide possible solutions and

---

[19]U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP, Exposure Draft (Washington, D.C.: Mar. 15, 2002).

recommendations.[20] Second, we have issued various guides to assist CIOs in tackling the major challenges that they have cited. This guidance includes (1) information security best practices to help agencies with their information security challenges;[21] (2) an IT investment management framework, including a new version that offers organizations a road map for improving their IT investment management processes in a systematic and organized manner;[22] and (3) a framework that provides agencies with a common benchmarking tool for planning and measuring their efforts to improve their enterprise architecture management.[23]

In summary, the report we are issuing today indicates that CIOs generally stated that they had most of the responsibilities and reporting relationships required by law, but that there were notable exceptions. In particular, some agency CIOs reported that, contrary to the requirements in the law, they were not responsible for certain areas, such as records management, and that they did not report to their agency head. However, views were mixed as to whether CIOs could be effective leaders without having responsibility for each individual area. In addition, most CIOs did

---

[20]See U.S. General Accounting Office, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 1 2004), *Human Capital: Selected Agencies' Experiences and Lessons Learned in Designing Training and Development Programs*, GAO-04-291 (Washington, D.C.: Jan. 30, 2004), *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003), *Human Capital: Insights for U.S. Agencies from Other Countries' Succession Planning and Management Initiatives,* GAO-03-914 (Washington, D.C.: Sept. 15 , 2003), *Human Capital: Opportunities to Improve Executive Agencies' Hiring Processes*, GAO-03-450 (Washington, D.C.: May 30, 2003), *Human Capital: OPM Can Better Assist Agencies in Using Personnel Flexibilities*, GAO-03-428 (Washington, D.C.: May 9, 2003), and *Information Technology Training: Practices of Leading Private-Sector Companies*, GAO-03-390 (Washington, D.C.: Jan. 31, 2003).

[21]U.S. General Accounting Office, *Executive Guide: Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1, 1998) and *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: Nov. 1, 1999).

[22]U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, GAO-04-394G (Washington, D.C.: Mar. 1, 2004). See also, U.S. General Accounting Office, *Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments*, GAO/AIMD-98-89 (Washington, D.C.: Mar. 1, 1998).

[23]U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1),* GAO-03-584G (Washington, D.C.: Apr. 1, 2003).

not stay in office for 3 to 5 years—the response most commonly given when we asked current CIOs and former agency IT executives how long a CIO needed to be in office to be effective. Agencies' use of various mechanisms, such as human capital flexibilities, could help reduce the turnover rate or mitigate its effect. Reducing turnover among CIOs is important because the amount time CIOs are in office can affect their ability to successfully address the major challenges they face. Some of these challenges—such as how IT projects are originated—may not be wholly within their control. Other challenges—such as improved IT management—are more likely to be overcome if a CIO has sufficient time to more effectively address these issues.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions that you or other Members of the Subcommittee may have at this time.

Legislative Evolution of Agency Chief Information Officer Roles and Responsibilities

For more than 20 years, federal law has structured the management of information technology and information-related activities under the umbrella of information resources management (IRM).[1] Originating in the 1977 recommendations of the Commission on Federal Paperwork, the IRM approach was first enacted into law in the Paperwork Reduction Act of 1980 (PRA).[2] The 1980 act focused primarily on centralizing governmentwide responsibilities in the Office of Management and Budget (OMB). The law gave OMB specific policy-setting and oversight duties with regard to individual IRM areas—for example, records management, privacy, and the acquisition and use of automatic data processing and telecommunications equipment (later renamed information technology). The law also gave agencies the more general responsibility to carry out their IRM activities in an efficient, effective, and economical manner and to comply with OMB policies and guidelines. To assist in this effort, the law required that each agency head designate a senior official who would report directly to the agency head to carry out the agency's responsibilities under the law.

Together, these requirements were intended to provide for a coordinated approach to managing federal agencies' information resources. The requirements addressed the entire information life cycle, from collection through disposition, in order to reduce information collection burdens on the public and to improve the efficiency and effectiveness of government.

Amendments to the PRA in 1986 and 1995 were designed to strengthen agency and OMB implementation of the law. Most particularly, the PRA of 1995 provided detailed agency requirements for each IRM area, to match the specific OMB provisions. The 1995 act also required for the first time that agencies develop processes to select, control, and evaluate the results of major information systems initiatives.

In 1996, the Clinger-Cohen Act supplemented the information technology management provisions of the PRA with detailed Chief Information Officer (CIO) requirements for IT capital planning and investment control and for

---

[1]IRM is the process of managing information resources to accomplish agency missions and to improve agency performance.

[2]P.L. 96-511, December 11, 1980.

performance and results-based management.[3] The 1996 act also established the position of agency chief information officer by amending the PRA to rename the senior IRM officials CIOs and by specifying additional responsibilities for them. Among other things, the act required IRM to be the "primary duty" of the CIOs in the 24 major departments and agencies specified in 31 U.S.C. 901. Accordingly, under current law,[4] agency CIOs are required to carry out the responsibilities of their agencies with respect to information resources management, including

- information collection and the control of paperwork;

- information dissemination;

- statistical policy and coordination;

- records management;

- privacy, including compliance with the Privacy Act;

- information security, including compliance with the Federal Information Security Management Act;

- information disclosure, including compliance with the Freedom of Information Act; and

- information technology.

---

[3]P.L. 104-106, February 10, 1996. The law, initially entitled the Information Technology Management Reform Act (ITMRA), was subsequently renamed the Clinger-Cohen Act in P.L. 104-208, September 30, 1996.

[4]The E-Government Act of 2002 reiterated agency responsibility for information resources management. P.L. 107-347, December 17, 2002.

Together, these legislated roles and responsibilities embody the policy 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.