

GAO

Report to the Committee on Homeland  
Security and Governmental Affairs,  
U.S. Senate

September 2011

FEDERAL CHIEF  
INFORMATION  
OFFICERS

Opportunities Exist to  
Improve Role in  
Information  
Technology  
Management

U.S. Government Accountability Office

GAO90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

Highlights of [GAO-11-634](#), a report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

The federal government invests billions in information technology (IT) each year to help agencies accomplish their missions. Federal law, particularly the Clinger-Cohen Act of 1996, has defined the role of Chief Information Officer (CIO) as the focal point for IT management within agencies. Given the longstanding challenges the government faces in managing IT and the continued importance of the CIO, GAO was asked to (1) determine the current roles and responsibilities of CIOs, (2) determine what potential modifications to the Clinger-Cohen Act and related laws could be made to enhance CIOs' authority and effectiveness, and (3) identify key lessons learned by CIOs in managing IT. To do this, GAO administered a questionnaire to 30 CIOs, compared responses to legislative requirements and the results of a 2004 GAO study, interviewed current CIOs, convened a panel of former agency CIOs, and spoke with the Office of Management and Budget's (OMB) Federal CIO.

## What GAO Recommends

GAO is recommending that OMB update its guidance to establish measures of accountability for ensuring that CIOs' responsibilities are fully implemented and require agencies to establish internal processes for documenting lessons learned. In commenting on a draft of this report, OMB officials generally agreed with GAO's findings and stated that OMB had taken actions that they believed addressed the recommendations.

View [GAO-11-634](#) or key components. For more information, contact Valerie C. Melvin at (202) 512-6304 or [melvinv@gao.gov](mailto:melvinv@gao.gov).

# FEDERAL CHIEF INFORMATION OFFICERS

## Opportunities Exist to Improve Role in Information Technology Management

## What GAO Found

CIOs do not consistently have responsibility for 13 major areas of IT and information management as defined by law or deemed as critical to effective IT management, but they have continued to focus more attention on IT management-related areas. Specifically, most CIOs are responsible for seven key IT management areas: capital planning and investment management; enterprise architecture; information security; IT strategic planning, "e-government" initiatives; systems acquisition, development, and integration; and IT workforce planning. By contrast, CIOs are less frequently responsible for information management duties such as records management and privacy requirements, which they commonly share with other offices or organizations within the agency. In this regard, CIOs report spending over two-thirds of their time on IT management responsibilities, and less than one-third of their time on information management responsibilities. CIOs also report devoting time to other responsibilities such as addressing infrastructure issues and identifying emerging technologies. Further, many CIOs serve in positions in addition to their role as CIO, such as human capital officer. In addition, tenure at the CIO position has remained at about 2 years. Finally, just over half of the CIOs reported directly to the head of their respective agencies, which is required by law. The CIOs and others have stressed that a variety of reporting relationships in an agency can be effective, but that CIOs need to have access to the agency head and form productive working relationships with senior executives across the agency in order to carry out their mission.

Federal law provides CIOs with adequate authority to manage IT for their agencies; however, some limitations exist that impede their ability to exercise this authority. Current and former CIOs, as well as the Federal CIO, did not identify legislative changes needed to enhance CIOs' authority and generally felt that existing law provides sufficient authority. Nevertheless, CIOs do face limitations in exercising their influence in certain IT management areas. Specifically, CIOs do not always have sufficient control over IT investments, and they often have limited influence over the IT workforce, such as in hiring and firing decisions and the performance of component-level CIOs. More consistent implementation of CIOs' authority could enhance their effectiveness in these areas. OMB has taken steps to increase CIOs' effectiveness, but it has not established measures of accountability to ensure that responsibilities are fully implemented.

CIOs identified a number of best practices and lessons learned for more effectively managing IT at agencies, and the Federal CIO Council has established a website to share this information among agencies. Agencies have begun to share information in the areas of vendor communication and contract management; the consolidation of multiple systems into an enterprise solution through the use of cloud services; and program manager development. However, CIOs have not implemented structured agency processes for sharing lessons learned. Doing so could help CIOs share ideas across their agencies and with their successors for improving work processes and increasing cost effectiveness.

---

# Contents

---

Letter		1
	Background	4
	Current Agency CIOs Do Not Have Responsibility for All Assigned Areas	18
	Federal Law Provides Adequate Authority, but Limitations Exist in Implementation for IT Management	28
	A Structured Process Could Improve Sharing of Lessons Learned within Agencies	33
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	40
Appendix II	Chief Information Officers Interviewed	43
Appendix III	Former Agency CIO Panel Participants	44
Appendix IV	Summary of CIOs' Information Management and Technology Responsibilities	45
Appendix V	CIO Tenure at Each Agency	58
Appendix VI	Comments from the Department of Defense	62
Appendix VII	Comments from the Department of Homeland Security	63
Appendix VIII	Comments from the Office of Personnel Management	64

## Tables

Table 1: Major Areas of CIO Responsibility in IT Management and Information Management	8
Table 2: Time Allocated as Reported by CIOs	22
Table 3: Comparison of Current CIO Backgrounds with Those of CIOs in 2004	26
Table 4: Comparison of CIO Tenure During 1996-2004 and 2004-2011	27
Table 5: Former Agency Chief Information Officer Panel	44
Table 6: Summary of CIO Responses to Questions on IT Strategic Planning	45
Table 7: Summary of CIO Responses to Questions for IT Workforce Planning	46
Table 8: Summary of CIO Responses to Questions for Capital Planning and Investment Management	47
Table 9: Summary of CIO Responses to Questions for Information Security	48
Table 10: Summary of CIO Responses to Questions for Enterprise Architecture	49
Table 11: Summary of CIO Responses to Questions on Systems Acquisition, Development, and Integration	50
Table 12: Summary of CIO Responses to Questions for E-government Initiatives	51
Table 13: Summary of CIO Responses to Questions on Information Collection/Paperwork Reduction	52
Table 14: Summary of CIO Responses to Questions for Information Dissemination	53
Table 15: Summary of CIO Responses to Questions on Information Disclosure	54
Table 16: Summary of CIO Responses to Questions for Statistical Policy and Coordination	55
Table 17: Summary of CIO Responses to Questions for Records Management	56
Table 18: Summary of CIO Responses to Questions for Privacy	57
Table 19: Statistical Analysis of CIO Tenure (2004-2011)	61

---

---

## Figures

Figure 1: Comparison of Number of CIOs Assigned Responsibility for IT Management and Information Management Areas between 2004 and 2011	21
Figure 2: CIO Tenure—Acting and Permanent	59
Figure 3: CIO Tenure—Career and Political Appointees	60

---

## Abbreviations

CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
IRM	information resources management
IT	information technology
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



**G A O**

Accountability \* Integrity \* Reliability

**United States Government Accountability Office**  
Washington, DC 20548

---

September 15, 2011

The Honorable Joseph I. Lieberman  
Chairman  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Susan M. Collins  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

In fiscal year 2011, the federal government estimates spending approximately \$79 billion for information technology (IT) investments. Although the government makes these substantial annual investments, it faces longstanding problems in its management of IT. Our most recent high-risk series update<sup>1</sup> continues to identify high-risk modernization efforts and governmentwide IT management challenges. Further, our recent report on opportunities to reduce potential duplication in government programs identified numerous areas in which IT programs could be consolidated or better managed to save taxpayer dollars and help agencies provide more efficient and effective services.<sup>2</sup>

Over the years, Congress has enacted various laws in an attempt to improve the government's performance in IT management. One of these laws—the Clinger-Cohen Act of 1996<sup>3</sup>—required agency heads to designate Chief Information Officers (CIO) to lead reforms that would help control system development risks; better manage technology spending; and achieve real, measurable improvements in agency performance. Additionally, we have long been proponents of having strong agency CIOs

---

<sup>1</sup>GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011).

<sup>2</sup>GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, [GAO-11-318SP](#) (Washington, D.C.: Mar. 1, 2011). An interactive, web-based version of the report is available at: <http://www.gao.gov/ereport/gao-11-318SP>.

<sup>3</sup>Div. E, P.L. 104-106, (Feb. 10, 1996); 40 U.S.C 11101, et seq. The law, initially titled the Information Technology Management Reform Act, was subsequently renamed the Clinger-Cohen Act in P.L. 104-208, (Sept. 30, 1996).

---

in place to lead federal agencies in managing IT. Recognizing the key role of CIOs in helping agencies achieve better results through IT, in July 2004, we reported our findings from a congressionally requested study that examined federal agency CIOs' roles and responsibilities, reporting relationships, tenure, and challenges.<sup>4</sup> That study, undertaken about 8 years following the enactment of the Clinger-Cohen Act, noted a number of findings regarding the extent to which CIOs had responsibilities for key IT management and other areas we identified as required by statute or as critical to IT management.<sup>5</sup> For example, we reported that few CIOs were responsible for all key IT and information management areas and generally reported to their agency heads or other top-level managers. Also, the CIOs had cited challenges in implementing effective IT management and obtaining sufficient and relevant resources, among others.

It has now been 15 years since enactment of the Clinger-Cohen Act, and recognizing the continued importance of the CIO position to achieving better results through IT management, you requested that we conduct a follow-up study of federal agency CIOs. As agreed, our objectives were to (1) determine the current roles and responsibilities of CIOs, (2) determine what potential modifications to the Clinger-Cohen Act and related laws could be made to enhance CIOs' authority and effectiveness, and (3) identify key lessons learned by CIOs in managing information technology.

To address these objectives, we administered a questionnaire to the CIOs of 30 federal departments and agencies (24 entities identified in the Chief Financial Officers Act, the 3 military departments, and 3

---

<sup>4</sup>GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, [GAO-04-823](#) (Washington, D.C.: July 21, 2004).

<sup>5</sup>These areas are IT strategic planning; IT workforce planning; capital planning and investment management; information security; information collection/paperwork reduction; information dissemination; information disclosure; statistical policy and coordination; records management; privacy; enterprise architecture; e-government initiatives; and systems acquisition, development, and integration.

---

independent federal agencies).<sup>6</sup> We asked CIOs about their roles and responsibilities, reporting relationships with the agency head, and changes needed to their authority and effectiveness in addressing areas of IT management. We also inquired about any experiences of these CIOs that could potentially serve as lessons learned in managing information technology. We then compared the questionnaire responses to statutory requirements for CIO roles and responsibilities. Further, we compared the overall findings with those in our 2004 report to identify any differences or trends in CIOs' responses. Subsequently, we conducted semi-structured interviews with each of the CIOs who were in office at the time of our review to corroborate and supplement information we received in the survey. In addition, we convened a panel of nine former federal CIOs to obtain their views on the roles and responsibilities of federal CIOs, based on their prior experiences serving in the position. Finally, we met with the Federal CIO to discuss IT reform initiatives being undertaken by the Office of Management and Budget (OMB) to enhance and clarify the roles of federal CIOs.

We conducted this performance audit at the 30 agencies and OMB from June 2010 to September 2011 in the Washington, D.C., metropolitan area in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more complete description of our objectives, scope, and methodology is provided in appendix I. The 30 CIOs and 9 former CIOs included in our study are identified in appendixes II and III, respectively.

---

<sup>6</sup>The 30 agencies covered by this report were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; 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 the U.S. Agency for International Development; the Air Force, the Army, and the Navy; and the Corporation for National and Community Service, the Commodity Futures Trading Commission, and the Federal Labor Relations Authority.



---

## Background

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 has presented longstanding challenges to agencies, and despite substantial IT investments, the federal government's management of IT has produced mixed results. The CIO position was established by Congress to serve as a focal point for IT within an agency to address these challenges.

---

## Legislative Evolution of Agency CIO Roles and Responsibilities

Since 1980, federal law has placed the management of IT under the umbrella of information resources management (IRM).<sup>7</sup> Originating in a 1977 recommendation to Congress from the Commission on Federal Paperwork, the IRM approach was first enacted into law in the Paperwork Reduction Act of 1980.<sup>8</sup> This act required OMB to oversee federal agency IRM areas, which combined IT with information management areas, including information collection, records management, and privacy.<sup>9</sup> The law also gave agencies a 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 IRM responsibilities of the agency under the law.

Amendments to the Paperwork Reduction Act in 1986 and 1995 were designed to strengthen agency and OMB implementation of the law.<sup>10</sup> Most particularly, the act's 1995 amendments provided detailed agency requirements for each IRM area, to match the specific OMB provisions.<sup>11</sup> In addition, these amendments required agencies to develop, for the first time, processes to select, control, and evaluate the results of major information systems initiatives.<sup>12</sup> Under the Paperwork Reduction Act, as

---

<sup>7</sup>IRM is the process of managing information resources to accomplish agency missions and to improve agency performance.

<sup>8</sup>P.L. 96-511 (Dec. 11, 1980).

<sup>9</sup>The act required OMB to oversee the acquisition and use of automatic data processing and telecommunications equipment (which later came to be known as IT).

<sup>10</sup>Title VIII, P.L. 99-591 (Oct. 30, 1986); P.L. 104-13 (May 22, 1995).

<sup>11</sup>44 U.S.C. 3506.

<sup>12</sup>44 U.S.C. 3506 (h)(5).

---

amended through 1995, senior IRM officials were required to carry out the responsibilities of their agencies with respect to IRM and report directly to the head of the agency.

In 1996, the Clinger-Cohen Act supplemented the information technology management provisions of the Paperwork Reduction Act with detailed requirements for IT capital planning and investment control and performance and results-based management.<sup>13</sup> The Clinger-Cohen Act also established the position of agency CIO by amending the Paperwork Reduction Act to rename the senior IRM officials “chief information officers” and specifying additional responsibilities for them.<sup>14</sup>

Accordingly, agency CIOs are required by law to carry out the responsibilities of their agencies with respect to

- information collection and control of paperwork;
- information dissemination;
- statistical policy and coordination;
- records management;
- privacy, including compliance with the Privacy Act;<sup>15</sup>
- information security, including compliance with the Federal Information Security Management Act (FISMA);<sup>16</sup>
- information disclosure, including compliance with the Freedom of Information Act (FOIA);<sup>17</sup> and
- information technology management.

---

<sup>13</sup>40 U.S.C. 11312 and 11313.

<sup>14</sup>40 U.S.C. 11315 and 44 U.S.C. 3506(a). The Clinger-Cohen Act requirement that agency CIOs have IRM as their primary duty applies to the 24 major departments and agencies listed in 31 U.S.C. 901(b). The E-Government Act of 2002 reiterated agency responsibility for information resources management. P.L. 107-347 (Dec. 17, 2002).

<sup>15</sup>5 U.S.C. 552a.

<sup>16</sup>44 U.S.C. 3541, et seq.

<sup>17</sup>5 U.S.C. 552.

---

Specifically, with regard to IT management, the CIO is responsible for

- implementing and enforcing applicable governmentwide and agency IT management policies, principles, standards, and guidelines;
- assuming responsibility and accountability for IT investments;
- assuming responsibility for maximizing the value and assessing and managing the risks of IT acquisitions through a process that, among other things, is integrated with budget, financial, and program management decisions, and provides for the selection, management, and evaluation of IT investments;
- establishing goals for improving the efficiency and effectiveness of agency operations through the effective use of IT;
- developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture; and
- monitoring the performance of IT programs and advising the agency head whether to continue, modify, or terminate such programs.

Together, these statutory responsibilities require CIOs to be key leaders in managing IT and other information functions in a coordinated fashion in order to improve the efficiency and effectiveness of programs and operations.

---

## Prior Reports on CIOs' Roles and Responsibilities

We have previously reported on the status of agency CIOs, including their roles and responsibilities, reporting relationships, backgrounds, and challenges. We have also reported on private-sector CIO roles and responsibilities and challenges and compared them with those of federal CIOs.

In October 1997, we testified on an OMB evaluation of the status of agency CIO appointments at 27 federal agencies shortly after enactment of the Clinger-Cohen Act.<sup>18</sup> In that testimony, we noted that OMB had identified several agencies where the CIO's duties, qualifications, and

---

<sup>18</sup>GAO, *Chief Information Officer: Ensuring Strong Leadership and an Effective Council*, GAO/T-AIMD-98-22 (Washington D.C.: Oct. 27, 1997).

---

placement met the requirements of the Clinger-Cohen Act. According to OMB, these CIOs had experience, both operationally and technically, in leveraging the use of information technology, capital planning, setting and monitoring performance measures, and establishing service levels with technology users. However, OMB had expressed concerns about the number of other agencies that had acting CIOs, and about CIOs whose qualifications did not appear to meet the requirements of the Clinger-Cohen Act or who did not report directly to the head of the agency. We pointed out that OMB had also raised concerns about agencies where the CIOs had other major management responsibilities or where it was unclear whether the CIO's primary duty was the IRM function. Our testimony emphasized the importance of OMB following through on its efforts to assess CIO appointments and resolve outstanding issues. We noted that, despite the urgent need to deal with major challenges, including poor security management, and the need to develop, maintain, and facilitate integrated systems architectures to guide agencies' system development efforts, there were many instances of CIOs who had responsibilities beyond IRM. While some of these CIOs' additional responsibilities were minor, in many cases they included major duties, such as financial operations, human resources, procurement, and grants management. We stressed that asking the CIO to shoulder a heavy load of responsibilities would make it extremely difficult, if not impossible, for that individual to devote full attention to IRM issues.

In July 2004, we reported the results of our study, based on a questionnaire and interviews with CIOs at the same 27 major departments and agencies that OMB had previously evaluated.<sup>19</sup> Our study examined 13 major areas of CIO responsibilities—7 areas predominantly in IT management and 6 areas predominantly in information management, as defined by the relevant laws or deemed critical to the effective management of IT. These areas are described in table 1, along with the relevant source.

---

<sup>19</sup>[GAO-04-823](#).

**Table 1: Major Areas of CIO Responsibility in IT Management and Information Management**

<b>CIO responsibility</b>	<b>Description</b>
<b>IT management areas</b>	
IT strategic planning	CIOs are responsible for strategic planning for all information and information technology management functions [Paperwork Reduction Act].
IT workforce planning	CIOs are responsible for assessing agency information and IT workforce needs and developing strategies and plans for meeting those needs [Paperwork Reduction Act and Clinger-Cohen Act].
Capital planning and investment management	CIOs are responsible for a process for selecting, controlling, and evaluating IT investments to produce business value, reduce investment-related risks, and increase accountability and transparency in the investment decision-making process [Paperwork Reduction Act and Clinger-Cohen Act].
Information security	CIOs are responsible for ensuring agency compliance with requirements to protect information and systems [Paperwork Reduction Act, Federal Information Security Management Act, and Clinger-Cohen Act].
Enterprise architecture	CIOs are responsible for developing and maintaining an enterprise architecture—the business and technology blueprint that links an agency’s strategic plan to IT programs and supporting system implementations [Clinger-Cohen Act]. <sup>a</sup>
Systems acquisition, development, and integration	CIO IT management responsibilities should include a primary role in developing and enforcing policies for systems acquisition, development, and integration with existing systems [Paperwork Reduction Act and Clinger-Cohen Act].
E-government initiatives	CIOs are responsible for promoting the use of IT, including the Internet and emerging technologies, to improve the productivity, efficiency, and effectiveness of agency operations, programs, and services [Paperwork Reduction Act, Clinger-Cohen Act, E-Government Act].
<b>Information management areas</b>	
Information collection/paperwork reduction	CIOs are responsible for the review of agency information collection proposals to maximize utility and minimize public paperwork burdens [Paperwork Reduction Act].
Information dissemination	CIOs are responsible for ensuring that the agency’s information dissemination activities meet policy goals, such as timely and equitable public access to information [Paperwork Reduction Act].
Information disclosure	CIOs are responsible for ensuring appropriate information disclosure under the Freedom of Information Act [Paperwork Reduction Act].
Statistical policy and coordination	CIOs are responsible for agency statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes [Paperwork Reduction Act].
Records management	CIOs are responsible for ensuring that the agency implements and enforces the records management policies and procedures required by the Federal Records Act [Paperwork Reduction Act].
Privacy	CIOs are responsible for ensuring agency compliance with the Privacy Act and related laws [Paperwork Reduction Act].

Source: GAO analysis of applicable legislation.

<sup>a</sup>The Clinger-Cohen Act mandate for CIOs to develop and implement agencywide information technology architectures has been implemented under OMB guidance (consistent with GAO best practices) for the development and implementation of enterprise architectures.

---

Our study found that CIOs were not responsible for all of the information and IT management areas. Specifically, all CIOs were responsible for only 5 of the 13 areas, while less than half of the CIOs were assigned responsibility for information disclosure and statistical policy and coordination. Overall, the views of these CIOs were mixed as to whether they could be effective leaders without having responsibility for each individual area.

The 2004 study also examined the backgrounds and tenure of CIOs, noting that they had a wide variety of prior experiences, but generally had work or educational backgrounds in IT or IT-related fields, as well as business knowledge related to their agencies. The CIOs and former agency IT executives in the study believed it was necessary for a CIO to stay in office for 3 to 5 years to be effective. However, at the time of our study, the median tenure of permanent CIOs whose time in office had been completed was about 2 years.

Based on the study, we also reported on major challenges that the federal CIOs said they faced in fulfilling their duties. In this regard, over 80 percent of the CIOs had cited implementing effective IT management and obtaining sufficient and relevant resources as challenges. We stressed that effectively tackling these reported challenges could improve the likelihood of a CIO's success. Further, we highlighted the opportunity for Congress to consider whether the existing statutory requirements related to CIO responsibilities and reporting to the agency head reflected the most effective assignment of information and technology management responsibilities and reporting relationships.

In September 2005,<sup>20</sup> we reported on the results of our study of 20 CIOs of leading private-sector companies.<sup>21</sup> We noted that most of the private-sector CIOs had full or shared responsibility for 9 of 12 functional areas

---

<sup>20</sup>GAO, *Chief Information Officers: Responsibilities and Information Technology Governance at Leading Private-Sector Companies*, [GAO-05-986](#) (Washington, D.C.: September 14, 2005).

<sup>21</sup>We visited companies recognized as leaders in IT management. In addition, we chose companies that performed activities similar to those performed by federal agencies (e.g. supply chain management, education, and income security). The companies visited included Walmart, International Business Machines, and General Motors.

---

that we had explored.<sup>22</sup> For the most part, the responsibilities assigned to these private-sector CIOs were similar to those assigned to federal CIOs. In only three areas (information dissemination and disclosure, information collection, and statistical policy) did half or fewer of the CIOs have responsibility. In 4 of the 12 functional areas, the difference between the private-sector CIOs and federal CIOs was greater.<sup>23</sup> Fewer of the private-sector CIOs had these responsibilities in each case. We also reported that private-sector CIOs faced challenges related to increasing IT's contribution to their organization's bottom line—such as controlling IT costs, increasing IT efficiencies, and using technology to improve business processes.

---

## Prior GAO Reports Identified Challenges within IT and Information Management

### Information Technology Management

Although agencies have taken constructive steps to improve IT and information management policies and practices, including through activities of CIOs, we have continued to identify and report on long-standing challenges in the key areas addressed in this report.

*IT strategic planning:* In January 2004,<sup>24</sup> we reported on the status of agencies' plans for applying information resources to improve the productivity, efficiency, and effectiveness of government programs. At that time, we noted that agencies generally had IT strategic plans that addressed elements such as information security and enterprise architecture, but did not cover key areas specified in the Paperwork Reduction Act. Agencies cited a variety of reasons for not having addressed these areas, including that the CIO position had been vacant, that not including a requirement in guidance was an oversight, or that the process was being revised. We pointed out that, not only are these practices based on law, executive orders, OMB policies, and our guidance, but they are also important ingredients for ensuring effective

---

<sup>22</sup>We reduced the 13 areas reviewed in the federal CIO study to 12 in the private-sector study by combining information dissemination and information disclosure into a single function. In addition, we treated e-government in the public sector as equivalent to e-business/e-commerce in the private sector.

<sup>23</sup>These areas were enterprise architecture, strategic planning, information collection, and information dissemination and disclosure.

<sup>24</sup>GAO, *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, [GAO-04-49](#) (Washington, D.C.: Jan. 12, 2004).

---

strategic planning, performance measurement, and investment management, which, in turn, make it more likely that the billions of dollars in government IT investments will be wisely spent. We made a number of recommendations, including that each agency take action to address IT strategic planning, performance measurement, and investment management practices that were not fully in place.

*IT workforce planning:* In 1994 and 2001,<sup>25</sup> we reported on the importance that leading organizations placed on making sure they had the right mix of skills in their IT workforce. In our 2004 report on CIOs' roles and responsibilities,<sup>26</sup> 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 February 2011, we identified strategic human capital management as a governmentwide high-risk area after finding that the lack of attention to strategic human capital planning had created a risk to the federal government's ability to serve the American people effectively.<sup>27</sup> As our previous reports have made clear, the widespread lack of attention to strategic human capital management in the past has created a fundamental weakness in the federal government's ability to perform its missions economically and efficiently.

*Capital planning and investment management:* Since 2002, using our investment management framework,<sup>28</sup> we have reported on the varying extents to which federal agencies have implemented sound practices for managing their IT investments. In this regard, we identified agencies that have made significant improvements by using the framework in implementing capital planning processes. In contrast, however, we have continued to identify weaknesses at agencies in many areas, including immature management processes to support both the selection and

---

<sup>25</sup>GAO, *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology*, [GAO/AIMD-94-115](#) (Washington, D.C.: May 1, 1994); and *Executive Guide: Maximizing the Success of Chief Information Officers: Learning From Leading Organizations*, [GAO-01-376G](#) (Washington, D.C.: Feb. 1, 2001).

<sup>26</sup>[GAO-04-823](#).

<sup>27</sup>[GAO-11-278](#).

<sup>28</sup>GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004).



---

oversight of major IT investments and the measurement of actual versus expected performance in meeting established performance measures.<sup>29</sup> For example, in 2007, we reported that two agencies did not have the processes in place to effectively select and oversee their major investments.<sup>30</sup> In June 2009,<sup>31</sup> we reported that about half of the projects we examined at 24 agencies did not receive selection reviews (to confirm that they support mission needs) or oversight reviews (to ensure that they were meeting expected cost and schedule targets). Specifically, 12 of the 24 reviewed projects that were identified by OMB as being poorly planned did not receive a selection review, and 13 of 28 poorly performing projects we examined had not received an oversight review by a department-level oversight board. Accordingly, we made recommendations to multiple agencies to ensure that the projects identified in the report as not having received oversight reviews received them.

*Information security:* Our reviews have noted significant information security control deficiencies that place agency operations and assets at risk. In addition, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. To address these and other challenges, we have recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings in risk assessments, information security policies and procedures, security planning, security

---

<sup>29</sup>For example, GAO, *Information Technology: Treasury Needs to Strengthen Its Investment Board Operations and Oversight*, [GAO-07-865](#) (Washington, D.C.: Jul. 23, 2007); *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, [GAO-07-424](#) (Washington, D.C.: Apr. 27, 2007); *Information Technology: Centers for Medicare & Medicaid Services Needs to Establish Critical Investment Management Capabilities*, [GAO-06-12](#) (Washington, D.C.: Oct. 28, 2005); *Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior*, [GAO-03-1028](#) (Washington, D.C.: Sept. 12, 2003); and *United States Postal Service: Opportunities to Strengthen IT Investment Management Capabilities*, [GAO-03-3](#) (Washington, D.C.: Oct. 15, 2002).

<sup>30</sup>[GAO-07-424](#) and [GAO-07-865](#).

<sup>31</sup>GAO, *Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects*, [GAO-09-566](#) (Washington, D.C.: June 30, 2009).

---

training, system tests and evaluations, and remedial actions. Due to the persistent nature of information security vulnerabilities and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress,<sup>32</sup> a designation we have made in each report since 1997.

*Enterprise architecture:* We have reported on the status of major federal department and agency enterprise architecture efforts.<sup>33</sup> We found that the state of the enterprise architecture programs at the major federal departments and agencies was mixed, with several having very immature programs, several having more mature programs, and most being somewhere in between. Collectively, agencies faced barriers or challenges in implementing their enterprise architectures, such as overcoming organizational parochialism and cultural resistance, having adequate resources (human capital and funding), and fostering top management understanding. To assist the agencies in addressing these challenges, we have made numerous recommendations aimed at ensuring that their respective enterprise architecture programs develop and implement plans for fully satisfying each of the conditions in our enterprise architecture management maturity framework.<sup>34</sup> In addition, in our most recent high-risk update report<sup>35</sup> we identified possible areas where enterprise architecture could help to alleviate some challenges. For example, we suggested that one agency align its corporate architecture and its component organization architectures to avoid investments that provide similar but duplicative functionality.

*Systems acquisition, development, and integration:* Our work has shown that applying rigorous practices to the acquisition or development of IT systems or the acquisition of IT services can improve the likelihood of success. In addition, we have identified leading commercial practices for outsourcing IT services that government entities could use to enhance their

---

<sup>32</sup>[GAO-11-278](#).

<sup>33</sup>GAO, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, [GAO-06-831](#) (Washington, D.C.: Aug. 14, 2006).

<sup>34</sup>GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 2.0), [GAO-10-846G](#) (Washington, D.C.: August 2010).

<sup>35</sup>[GAO-11-278](#).

---

acquisition of IT systems and services.<sup>36</sup> We have evaluated several agencies' software development or acquisition processes and reported that agencies are not consistently using rigorous or disciplined system management practices.<sup>37</sup> For example, after reviewing the Department of Homeland Security's Atlas investment,<sup>38</sup> we recommended that the agency implement effective management controls and capabilities by, among other things, revising and updating its cost-benefit analysis; making the program office operational; developing and implementing rigorous performance program management practices; and ensuring plans fully disclose the system capabilities, schedule, cost, and benefits to be delivered. In addition, ensuring that effective system acquisition management controls are implemented on each agency business system investment remains a formidable challenge, as our recent reports on management weaknesses associated with individual programs have demonstrated. For example, we recently reported that the Department of Defense's large-scale software-intensive system acquisitions continued to fall short of cost, schedule, and performance expectations.<sup>39</sup> Specifically, our report noted that six of the department's nine enterprise resource planning systems had experienced schedule delays ranging from 2 to 12 years, and five had incurred cost increases ranging from \$530 million to \$2.4 billion.

*E-government initiatives:* In December 2004, we reported the results of our review of the implementation status of major provisions from the E-Government Act of 2002,<sup>40</sup> which required a wide range of activities across the federal government aimed at promoting electronic government, such as providing the public with access to government information and services. We found that, although the government had

---

<sup>36</sup>GAO, *Information Technology: Leading Commercial Practices for Outsourcing of Services*, [GAO-02-214](#) (Washington, D.C.: Nov. 30, 2001).

<sup>37</sup>For example, see GAO, *Information Technology: Inconsistent Software Acquisition Processes at the Defense Logistics Agency Increase Project Risks*, [GAO-02-9](#) (Washington, D.C.: Jan. 10, 2002); and *HUD Information Systems: Immature Software Acquisition Capability Increases Project Risks*, [GAO-01-962](#) (Washington, D.C.: Sept. 14, 2001).

<sup>38</sup>GAO, *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program*, [GAO-05-805](#) (Washington, D.C.: Sept. 7, 2005).

<sup>39</sup>[GAO-11-278](#).

<sup>40</sup>GAO, *Electronic Government: Federal Agencies Have Made Progress Implementing the E-Government Act of 2002*, [GAO-05-12](#) (Washington, D.C.: Dec. 10, 2004).

---

made progress in implementing the act, the act's requirements were not always fully addressed. Specifically, OMB had not (1) ensured that a study on using IT to enhance crisis preparedness and response had been conducted that addressed the content specified by the act, (2) established a required program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic government services and processes, or (3) ensured the development and maintenance of a required repository and website of information about research and development funded by the federal government. We made recommendations to OMB aimed at ensuring more consistent implementation of the act's requirements.

## Information Management

We have also reported on various challenges agencies faced in meeting information management requirements, including in the areas of privacy, information collection, records management, information disclosure, and information dissemination.

In 2002 and 2003, we reported on agencies' handling of the personal information they collect and whether this handling conforms to the Privacy Act and other laws and guidance. In the 2002 report, we made recommendations to selected agencies aimed at strengthening their compliance with privacy requirements.<sup>41</sup> In the 2003 report, we made recommendations to OMB, which included directing agencies to correct compliance deficiencies, monitoring agency compliance, and reassessing OMB guidance.<sup>42</sup>

In 2005, we reviewed agency compliance with information collection clearance requirements under the Paperwork Reduction Act.<sup>43</sup> In an analysis of 12 case studies, we found that while CIOs generally reviewed information collections and certified that they met the standards in the act, in a significant number of instances, agencies did not provide support for the certifications, as the law requires. We recommended that OMB and

---

<sup>41</sup>GAO, *Information Management: Selected Agencies' Handling of Personal Information*, [GAO-02-1058](#) (Washington, D.C.: September 30, 2002).

<sup>42</sup>GAO, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, [GAO-03-304](#) (Washington, D.C.: June 30, 2003).

<sup>43</sup>GAO, *Paperwork Reduction Act: New Approach May Be Needed to Reduce Government Burden on Public*, [GAO-05-424](#) (Washington, D.C.: May 2005).

---

the agencies take steps to improve review processes and compliance with the act.

In 2008, we reviewed the management of e-mail records at four agencies and found agency practices did not always conform to requirements. We recommended that the National Archives and Records Administration develop and implement an oversight approach that provides adequate assurance that agencies are following its guidance, including both regular assessments of agency records and records management programs and reporting on these assessments.<sup>44</sup>

Also in 2008, we reported on trends in Freedom of Information Act processing and agencies' progress in addressing backlogs of overdue FOIA requests.<sup>45</sup> We found weaknesses in agency reporting on FOIA processing and recommended, among other things, that guidance be improved for agencies to track and report on overdue requests and plans to meet future backlog goals.

In July 2010, we identified and described current uses of web 2.0 technologies by federal agencies to disseminate information.<sup>46</sup> Specifically, we found that the federal government may face challenges in determining how to appropriately limit collection and use of personal information as agencies utilize these technologies and how and when to extend privacy protections to information collected and used by third-party providers of web 2.0 services. In July 2011, we identified ways agencies are using social media to interact with the public and assessed the extent to which they had policies in place for managing and identifying records, protecting personal information, and ensuring the security of federal information and systems. We made recommendations to 21 agencies to improve their development and implementation of social media policies.<sup>47</sup>

---

<sup>44</sup>GAO, *Federal Records: National Archives and Selected Agencies Need to Strengthen E-Mail Management*, [GAO-08-742](#) (Washington, D.C.: June 13, 2008).

<sup>45</sup>GAO, *Freedom Of Information Act: Agencies Are Making Progress in Reducing Backlog, but Additional Guidance Is Needed*, [GAO-08-344](#) (Washington, D.C.: March 14, 2008).

<sup>46</sup>GAO, *Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies*, [GAO-10-872T](#) (Washington, D.C.: July 22, 2010).

<sup>47</sup>GAO, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, [GAO-11-605](#) (Washington, D.C.: Jun. 28, 2011).

---

## OMB Has Several Initiatives Under Way to Improve the Oversight and Management of IT, Including Changing the Role of Federal Agency CIOs

On March 5, 2009, President Obama designated the Administrator of OMB's Office of Electronic Government and Information Technology as the first Federal Chief Information Officer. The Federal CIO was given responsibility for directing the policy and strategic planning of federal information technology investments as well as for overseeing federal technology spending.

Toward this end, in December 2010, the Federal CIO issued a 25 Point Implementation Plan to Reform Federal Information Technology Management. This 18-month plan specified five major goals: strengthening program management, streamlining governance and improving accountability, increasing engagement with industry, aligning the acquisition process with the technology cycle, and applying "light technology" and shared solutions.<sup>48</sup> As part of this plan, OMB has initiatives under way to, among other things, strengthen agencies' investment review boards and to consolidate federal data centers. The plan stated that OMB will work with Congress to consolidate commodity IT spending (e.g., e-mail, data centers, content management systems, web infrastructure) under agency CIOs. Further, the plan called for the role of federal agency CIOs to focus more on IT portfolio management.

In March 2011, we testified on the efforts of OMB and the Federal CIO to improve the oversight and management of IT investments in light of the problems that agencies have continued to experience with establishing IT governance processes to manage such investments.<sup>49</sup> These initiatives included increasing the accountability of agency CIOs through the use of the IT Dashboard, a public website established in June 2009 that provides detailed information, including performance ratings, for over 800 major IT investments at federal agencies. Each investment's performance data are updated monthly, which is a major improvement from the quarterly reporting cycle used by OMB's prior oversight mechanisms. However, in a series of reviews, we have found that the data on the Dashboard were not always accurate. Specifically, we found that the

---

<sup>48</sup>This refers to services that can be deployed rapidly and solutions that will result in substantial cost savings, allowing agencies to optimize spending and reinvest in their most critical mission needs.

<sup>49</sup>GAO, *Information Technology: Investment Oversight and Management Have Improved but Continued Attention is Needed*, [GAO-11-454T](#) (Washington, D.C.: Mar. 17, 2011).

---

Dashboard ratings were not always consistent with agency performance data.<sup>50</sup>

OMB has also initiated efforts to improve the management of IT investments needing attention. In particular, in January 2010, the Federal CIO began leading TechStat sessions—a review of selected IT investments between OMB and agency leadership to increase accountability and transparency and improve performance. We noted that the full implementation of OMB’s 18-month roadmap should result in more effective IT management and delivery of mission-critical systems, as well as further reduction in wasteful spending on poorly managed investments.<sup>51</sup>

---

## Current Agency CIOs Do Not Have Responsibility for All Assigned Areas

Similar to 2004, we found that the CIOs are not consistently responsible for all of the 13 areas assigned by statute or identified as critical to effective IT management; however, they are more focused on IT management than on the management of agency information. The majority of CIOs (between 23 and 27)<sup>52</sup> reported they are responsible for the seven areas of IT management. In this regard, the CIOs reported being responsible for activities in managing IT that include the following:

- managing capital planning and investment management processes to ensure that they were successfully implemented and integrated with the agency’s budget, acquisition, and planning processes;
- developing, maintaining, and facilitating the implementation of sound and integrated enterprise architectures;
- designating a senior department official who will have responsibility for departmentwide information security;

---

<sup>50</sup>GAO, *Information Technology: OMB’s Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, [GAO-10-701](#) (Washington, D.C.: July 16, 2010) and *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy*, [GAO-11-262](#) (Washington, D.C.: Mar. 15, 2011).

<sup>51</sup>[GAO-11-454T](#).

<sup>52</sup>For comparison to our 2004 report, we did not include the three small, independent agencies in this count.

- 
- developing IT strategic plans to emphasize the role that IT can play in effectively supporting the department's operations and goals;
  - developing, maintaining, and improving systems acquisition processes;
  - managing e-government requirements and ensuring compliance with legislation; and
  - developing strategies for development of a skilled IT workforce combined with strong succession planning.

Fewer CIOs (between 6 and 22) reported being responsible for the six areas predominantly related to information management (information collection/paperwork reduction, records management, privacy, information dissemination, information disclosure, and statistical policy and coordination). Even those CIOs who indicated they had been assigned responsibility for these six information management areas reported they assigned a higher priority to their IT management responsibilities.

CIOs who reported they were not responsible for their agencies' information management functions said they provided input or other assistance to the organizational units within their agencies that were primarily responsible for these areas. The units with which they shared responsibilities varied, as did the roles the CIO played. For example, in the area of records management, one CIO reported working closely with the agency's data manager and making recommendations regarding records management. In the privacy area,<sup>53</sup> one CIO reported coordinating with the agency's Chief Information Security Officer, general counsel, and human resources offices to address any privacy issues. To ensure accuracy of information disseminated, one CIO reported collaborating with the agency's Office of Public Affairs.

---

<sup>53</sup>OMB Memorandum M-05-08 required agencies to designate a senior official who has the overall agencywide responsibility for information privacy issues. It further indicated that if the CIO is not designated as responsible for privacy, the agency may designate another senior official (at the Assistant Secretary or equivalent level) with agencywide responsibility for information privacy issues.



---

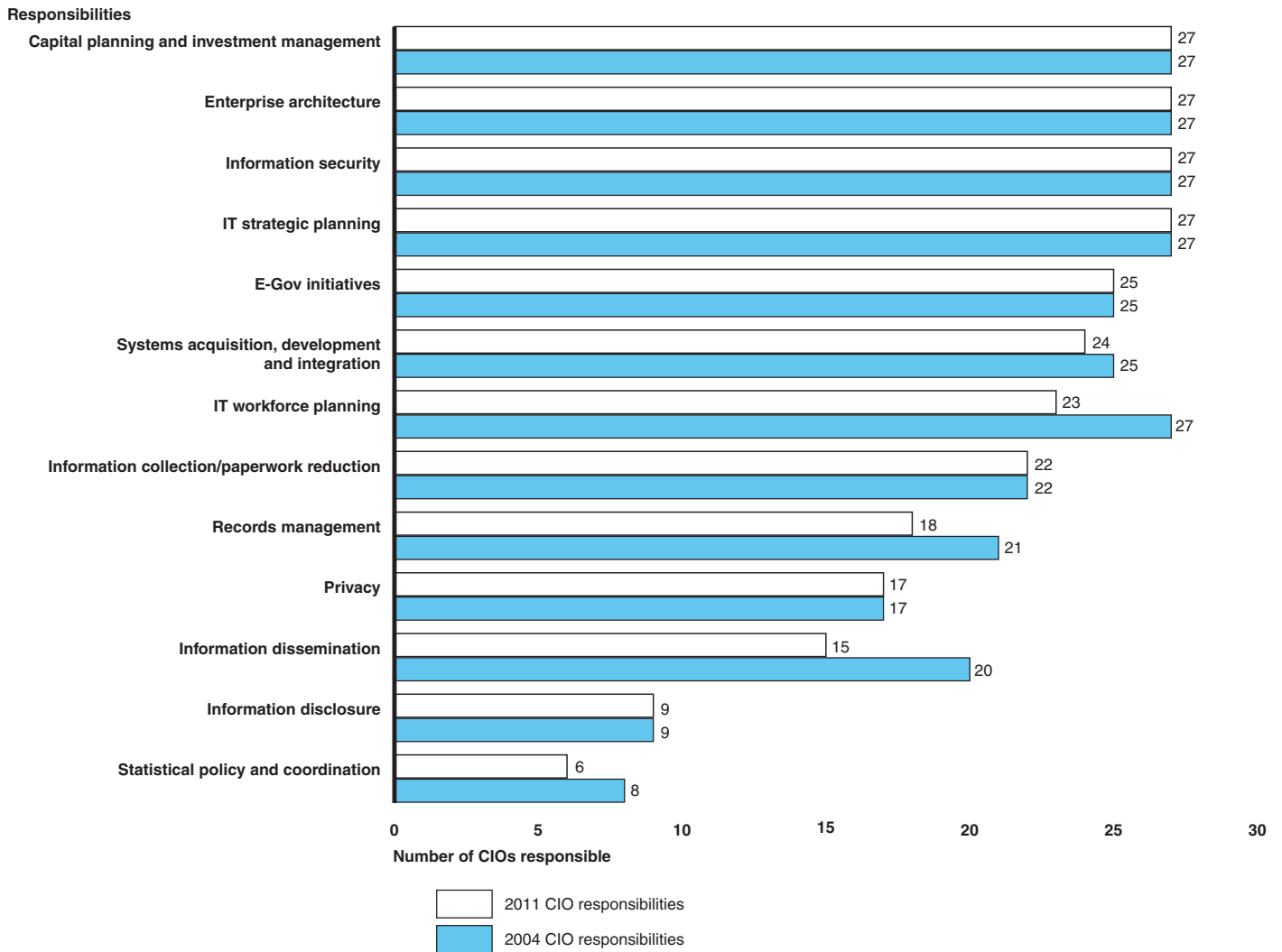
The areas in which the least number of CIOs reported they were responsible were statistical policy and coordination and information disclosure. In this regard, 21 CIOs stated that statistical policy and coordination was handled by other offices within their agencies, such as a policy or research office. This included components functioning as Principal Statistical Agencies.<sup>54</sup> Eighteen CIOs reported that responsibility for information disclosure rested with another office, such as an agency's FOIA office.

In comparison to 2004, the number of CIOs assigned responsibility for each of the areas remained the same for all but five areas (systems acquisition, development, and integration; IT workforce planning; records management; information dissemination; and statistical policy and coordination). In each of these areas, the number of CIOs assigned responsibility decreased from 2004 to 2011. Figure 1 shows the number of CIOs with responsibility for the 13 areas in 2011 and 2004.

---

<sup>54</sup>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 Program Development and Research (Social Security Administration), Office of Management and Budget (Executive Office of the President), and the U.S. Census Bureau (Department of Commerce).

**Figure 1: Comparison of Number of CIOs Assigned Responsibility for IT Management and Information Management Areas between 2004 and 2011**



Source: GAO analysis of agency-provided data.

Note: Excludes three small, independent agencies that were not included in our 2004 review.

## CIOs Spend the Majority of Their Time Managing Information Technology

The amount of time that CIOs spend in various areas of responsibility reflects their greater emphasis on IT management compared with the management of agency information. Specifically, CIOs reported they devote over two-thirds of their time to the seven IT management areas, which they generally viewed as more important to accomplishing their mission. Moreover, the majority of the CIOs were responsible for each of the areas.

By contrast, the CIOs reported spending less than one-fifth of their time in the six information management areas. Specifically, CIOs reported spending 6 percent or less of their time on average in each of the areas of privacy, e-government initiatives, records management, information dissemination, information collection/paperwork reduction, information disclosure, and statistical policy and coordination. As discussed previously, most CIOs reported they were not responsible for all of these areas and indicated they did not always place a high priority on them. This is consistent with the views held by the panel of former federal CIOs, which generally did not place high priority on the information management areas. Table 2 shows the percentage of time CIOs reported allocating to the 13 areas.

**Table 2: Time Allocated as Reported by CIOs**

IT management and information management areas	Average time allocated (% of time per week)
Information security	14%
Areas of responsibility outside the 13 areas	14
Capital planning and investment management	13
IT strategic planning	11
Systems acquisition, development, and integration	11
Enterprise architecture	9
IT workforce planning	7
Privacy	6
E-government initiatives	5
Records management	4
Information dissemination	3
Information collection/paperwork reduction	2
Information disclosure	2
Statistical policy and coordination	1

Source: GAO analysis of CIO responses.

Note: Percentages may not sum to 100 due to rounding.

---

The CIOs also reported they spend a significant amount of time outside the 13 areas of responsibility. Specifically, CIOs indicated they spend about 14 percent of their time on other responsibilities outside these 13 areas—the same amount of time as they spend on information security, the area where CIOs reported spending the most time. These additional areas of responsibility included addressing infrastructure issues,<sup>55</sup> participating in agencywide boards, or participating in external organizations, such as the federal CIO Council.<sup>56</sup>

In addition, CIOs reported they have begun to focus on emerging areas within IT such as cloud computing,<sup>57</sup> data center consolidation, and commodity services.<sup>58</sup> This is consistent with the recent emphasis of the Federal CIO on reforming IT, as reflected in OMB's IT Reform Plan. As technology continues to evolve, CIOs are likely to be challenged in ensuring that agencies use new technologies efficiently and effectively.

---

## Many CIOs Serve in Multiple Positions

An element that may potentially influence the likely success of an agency CIO is whether the CIO serves in any other agency position. According to the Clinger-Cohen Act, the CIO's statutory information and IT management functions should be that official's primary duties. We<sup>59</sup> and members of Congress<sup>60</sup> have previously expressed concern about agency CIOs having responsibilities beyond their primary duties and have questioned whether split duties allow a CIO to deal effectively with an agency's IT challenges.

---

<sup>55</sup>Infrastructure issues could refer to any problems with keeping an agency's core IT functions running, such as e-mail.

<sup>56</sup>The federal CIO Council is the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources.

<sup>57</sup>Cloud computing is an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies.

<sup>58</sup>This refers to systems used to carry out routine tasks (e.g., e-mail, data centers, web infrastructure).

<sup>59</sup>[GAO/T-AIMD-98-22](#).

<sup>60</sup>U.S. Senate Committee on Governmental Affairs, *Paperwork Reduction Act of 1995*, Senate Report 104-8 (Washington, D.C.: Jan. 30, 1995).

---

Despite the importance of focusing on their primary duties, the CIOs in our review reported holding a number of official agency job functions in addition to being CIO. Specifically, 14 of 30 CIOs reported serving in another position within their agency besides that of CIO. Of these, 11 reported that serving as CIO was their primary job function. Six of the 14 CIOs reported holding two or more positions besides CIO, with one holding five positions, including CIO. These positions included Chief Acquisition Officer and Chief Human Capital Officer.

Six of the 14 CIOs felt their other agency job positions were having a positive and helpful impact on their role as CIO. For example, one CIO, who also served as Deputy Chief of Staff, explained that holding the two positions showed staff a link between agency policy and operational implementation. According to another CIO, also holding the position of Chief Human Capital Officer provided insight into problems the agency had with a new personnel system. As a result, the CIO believed he was able to address these problems more quickly. The 8 remaining CIOs reported that their additional job functions had neither a positive nor negative impact on their role as a CIO, with one exception. Specifically, one CIO explained that having multiple positions had put a greater strain on the CIO's ability to adequately perform all required responsibilities. Holding other positions is contrary to the federal law requiring that IT and information management be the CIO's primary function and distracts from the responsibility to ensure that agencies carry out their IT and information management activities in an efficient, effective, and economical manner.

---

### CIOs Generally Report Directly to the Agency Head

Federal law calls for agency CIOs to report to the head of their agency. With regard to this requirement, we reported in 2004 that only 19 of 27 CIOs reported to their agency head, and views were mixed about whether such a direct reporting relationship was important. In our current study, even fewer—17 of 30—CIOs indicated that they report to their agency head, although 23 thought it was important to do so.

Despite this, the views of agency CIOs and others suggested that a variety of reporting relationships between an agency head and the CIO can be effective. CIOs generally agreed that access to the agency head was important, but that they did not necessarily require a formal reporting relationship. One said that it was important to have a “seat at the table” allowing for direct interaction with the agency head in order to articulate any problems or issues in IT.

---

However, other CIOs stated that it was important for the CIO to report to whomever is in charge of running the daily operations of the agency. One CIO did not believe it was ideal to report directly to the agency head because the agency head has too many other responsibilities. This CIO was able to meet with the agency's deputy secretary frequently and felt this resulted in more input into decision making. Another CIO, who reported to the agency head, believed there was not one ideal reporting relationship for the entire federal government because of the differences in size and mission among the agencies.

Two CIOs in our review indicated they did not have sufficient access to their agency head, even though they thought it was important to have such access. Accordingly, the CIOs felt they did not have sufficient influence on IT management decisions in their agency. The CIOs stated they had worked to gain greater influence over IT by establishing relationships with peers in their agencies such as the Chief Financial Officer or Chief Operating Officer.

Overall, regardless of the reporting relationship between agency heads and agency CIOs, 28 of the CIOs reported they had adequate access to their agency head. Additionally, many of the agency CIOs who did not report directly to the agency head indicated having influence on IT management decisions within their agency because they had relationships with other senior agency officials. These included direct reporting relationships with an assistant secretary or the Chief Operating Officer.

Based on their experiences, members of the panel of former CIOs stated that it was important to report to the agency head on key issues, but also to work with other senior officials for day-to-day activities. In this regard, the former CIOs believed it was essential for the CIO to forge relationships with other senior officials in an agency, such as the Chief Financial Officer and members of the Office of General Counsel. Further, in discussing this matter, the Federal CIO stated that reporting relationships should be determined on an agency-by-agency basis, noting that agencies should determine how best to meet this requirement depending on how the agency is structured. Given the varying responsibilities of agency heads and other senior officials, some degree of flexibility in CIOs' reporting relationships may be appropriate as long as CIO effectiveness is not impeded.

**CIOs’ Education and Work Experiences Remain Diverse, although More Have Previously Served as a CIO or Deputy CIO**

Although the qualifications of a CIO can help determine whether he or she is likely to be successful, there is no general agreement on the optimal background (e.g., education, experience) that a prospective agency CIO should have. The conference report accompanying the Clinger-Cohen Act stated that CIOs should possess knowledge of and practical experience in the information and IT management practices of business or government.<sup>61</sup> We found that when compared to CIOs in 2004, more current CIOs had served previously as a CIO or deputy CIO.

As shown in table 3 below, 18 of the CIOs in our review had experience as either a CIO or deputy CIO, an increase of 6 compared to the CIOs that participated in our 2004 review. Also, 21 current CIOs had previously worked for the federal government, 14 had worked in private industry, 4 had been in academia, and 4 had worked in state and local government. Fifteen CIOs had worked in some combination of two or more of these sectors. Further, all of the current CIOs had work experience in IT or IT-related fields.

**Table 3: Comparison of Current CIO Backgrounds with Those of CIOs in 2004**

Description	2004 CIOs	2011 CIOs
Number of CIOs who had served previously as a CIO or deputy CIO	12	18
Number of CIOs with federal government experience	24	21
Number of CIOs with private sector experience	16	14

Source: GAO analysis of agency data.

Note: This comparison does not include CIOs from the three small, independent agencies as they were not part of our 2004 review.

We asked current and former CIOs what key attributes they had found necessary to be an effective CIO. In response, they noted the need for IT experience and an understanding of how IT can be used to transform agencies and improve mission performance. Of most importance, however, were leadership skills and the ability to communicate effectively. The Federal CIO noted that he valued CIOs who thought about the future of the agency and demonstrated an ability to successfully manage IT programs or projects.

<sup>61</sup>House of Representatives, *National Defense Authorization Act for Fiscal Year 1996, Conference Report to Accompany S.1124*, House Report 104-450 (Washington, D.C.: Jan. 22, 1996).

## Median CIO Tenure Remains at About 2 Years

We noted previously that one element that influences the likely success of an agency CIO is the length of time the individual in the position has to implement change. For example, our prior work has noted that it can take 5 to 7 years to fully implement major change initiatives in large public and private sector organizations and to transform related cultures in a sustainable manner. Nonetheless, when we reported on this matter in 2004, the median tenure for permanent CIOs who had completed their time in office was just under 2 years.<sup>62</sup>

Tenure at the CIO position has remained almost the same since we last reported. Specifically, the median tenure for permanent federal agency CIOs was about 25 months for those who served between 2004 and 2011. However, the number of CIOs who stayed in office at least 3 years declined from 35 percent in 2004 to 25 percent in 2011.<sup>63</sup> (See table 4 for a comparison of CIO tenures from 1996 to 2004 and 2004 to 2011; see app. V for figures depicting the tenure for each of the CIOs at the agencies in our review between 2004 and 2011 and a table showing various statistical analyses on CIO tenure.)

**Table 4: Comparison of CIO Tenure During 1996-2004 and 2004-2011**

Description	1996-2004	2004-2011
Median tenure of CIOs (including current CIOs)	23 months	25 months
Percentage of CIOs who stayed in office for at least 3 years (excluding current CIOs)	35%	25%
Difference in median tenure between political and career CIOs (excluding current CIOs)	13 months	4 months

Source: GAO analysis of agency data.

We previously reported on factors that affected the tenure of CIOs, which included the stressful nature of the position and whether or not CIOs were political or career appointees. The panel of former CIOs for our current study agreed that high stress levels can lead to CIOs leaving the position, as can factors such as retirement and the opportunity to serve as a CIO at a larger agency. However, we found that during the period covered by

<sup>62</sup>Our last review included CIOs who were in office between February 10, 1996, and March 1, 2004. This review included CIOs who were in office between January 15, 2004, and March 15, 2011.

<sup>63</sup>This only included CIOs who had completed their time in office.



---

our current review, political appointees stayed only 4 months less than those in career civil service positions, compared to 13 months less in our 2004 review.

---

## Federal Law Provides Adequate Authority, but Limitations Exist in Implementation for IT Management

As previously discussed, a major goal of the Clinger-Cohen Act was to establish CIOs to advise and assist agency heads in managing IT investments. In this regard, the agency CIO was given the authority to administer a process to ensure that IT investments are selected, controlled, and evaluated in a manner that increases the likelihood they produce business value and reduce investment-related risk. As part of this process, CIOs are responsible for advising the agency head on whether IT programs and projects should be continued, modified, or terminated. In order to carry out these responsibilities, CIOs should be positioned within their agencies to successfully exercise their authority. Specifically, we have previously noted that CIOs should have a key role in IT investment decision making and budget control.<sup>64</sup> In addition, CIOs require visibility into and influence over programs, resources, and decisions related to the management of IT throughout the agency.

Our study did not find convincing evidence that specific legislative changes are needed to improve CIOs' effectiveness. Rather, we found that CIOs' ability to carry out their roles, as prescribed in law, has been limited by certain factors that have led to challenges. Specifically, CIOs reported they were hindered in exercising their authority over agency IT budgets, component IT spending, and staff, which our prior work has shown can lead to an inefficient use of funds.

*IT Budget authority:* Although assigned by law with the authority to be accountable for IT management, we found that CIOs faced limitations in their ability to influence IT investment decision making at their agencies. For example, only 9 CIOs responded that their approval was required for the inclusion of all IT investments in their agency's budget. The remaining 21 CIOs indicated that their explicit approval either was not required or it was required for major IT investments only.<sup>65</sup> Ten of those 21 CIOs

---

<sup>64</sup>[GAO/T-AIMD-98-22](#).

<sup>65</sup>This is referring to investments requiring an OMB exhibit 300. Each year, agencies submit to OMB a Capital Asset Plan and Business Case—the exhibit 300—to justify each request for a major information technology investment.

---

indicated they would be more effective if their explicit approval for IT investment decisions was sought by their agency head. CIOs said having this ability would reduce the number of unknown or “rogue” systems (i.e., systems not vetted by the CIO office), allow the CIO to identify and eliminate duplicative systems, and resolve technology and security issues earlier in an investment’s lifecycle. Further, 13 of the CIOs in our study did not have the power to cancel funding for IT investments. CIOs that did not have this power told us they would be more effective if they were able to cancel funding for investments because they would then be in a better position to consolidate investments and cut wasteful spending on failing projects.

In our previous reviews, we have noted limitations in CIOs’ ability to influence IT investments, which have contributed to long-standing challenges in agencies’ management of IT. For instance, we previously reported that one agency did not provide the department’s CIO with the level of IT spending control that our research at leading organizations and past work at federal departments and agencies have shown is important for effective integration of systems across organizational components.<sup>66</sup> We noted that control over the department’s IT budget was vested primarily with the CIO organizations within each of its component organizations. Consequently, there was an increased risk that component agencies’ ongoing investments would need to be reworked to be effectively integrated and maximize departmentwide value.

*Component-level IT spending:* A significant portion of an agency’s IT funding can be allocated and spent at the component level on commodity IT systems—systems used to carry out routine tasks (e.g., e-mail, data centers, web infrastructure)—in addition to mission-specific systems. Multiple CIOs faced limitations in their ability to influence agency decisions on integrating commodity IT systems throughout their agencies because they did not have control over funding for these systems at the component level. According to CIOs, more control over component-level IT funding, including commodity IT and mission-specific systems, could help ensure greater visibility into and influence on the effective acquisition and use of IT. Further, the Federal CIO has called for agencies to place all commodity IT purchases under the purview of the agency CIO, while

---

<sup>66</sup>GAO, *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, GAO-04-509 (Washington, D.C.: May 21, 2004).

---

component mission-specific systems should remain with the component CIO. OMB included centralization of commodity funding under agency CIOs as part of its current IT reform initiatives.

Consistent with this, we have reported on the importance of agency CIOs having adequate oversight to ensure that funds being spent on component agency investments will fulfill mission needs.<sup>67</sup> Specifically, at one agency, we found a structured mechanism was not in place for ensuring that component agencies defined and implemented investment management processes that were aligned with those of the department. Because such processes, including reviews of component agency IT investments, were not in place, the agency CIO did not have visibility into a majority of the agency's discretionary investments and could not ensure the agency's IT investments were maximizing returns.

*IT workforce:* CIOs also face limitations in their ability to provide input into hiring component-level senior IT managers and other IT staff. Many CIOs in our study faced limitations in performing certain workforce planning activities, such as having direct hiring capability for IT staff, providing input into the hiring of component CIOs, and influencing component agency CIOs' performance ratings. For example, some CIOs indicated they did not have any input into the hiring of their own staff. In addition, CIOs did not always participate in selections for candidate component CIOs. Further, for a majority of the agencies with component CIOs, the agency CIO did not participate in the component CIOs' performance reviews. Without sufficient influence over the hiring of IT staff or component CIOs' performance, agency CIOs are limited in their ability to ensure appropriate IT staff are being hired to meet mission needs or component accountability for overall agency priorities and objectives.

We have also previously reported on CIOs' challenges related to IT workforce planning, noting there has been a lack of attention in this area, which has created weaknesses in the federal government's ability to perform its missions economically, efficiently, and effectively.<sup>68</sup> In addition, in our previous review of CIOs' roles and responsibilities, we found that about 70 percent of CIOs reported IT workforce planning challenges within their agency. Without addressing CIOs' lack of influence

---

<sup>67</sup>[GAO-06-11](#).

<sup>68</sup>[GAO-04-823](#).

---

over IT workforce planning, the government will continue to face challenges in this area, risking further inefficiencies.

Most CIOs included in our study and the panel of former CIOs agreed that legislative changes were not needed to improve effectiveness in IT management. However, several CIOs told us their agencies have completed or initiated efforts to increase the influence of the CIO. For example, one agency gave its CIO complete control over the entire IT budget and all IT staff. This CIO told us that this has allowed for rapid, effective changes to be made when necessary on IT issues. Another agency began an agencywide consolidation effort so that the CIO's responsibility will be delegated to one person to centrally manage IT assets instead of multiple agency CIOs. This agency recently implemented a policy that has given one individual the title of CIO and stated that the CIO will assume oversight, management, ownership, and control of all departmental IT infrastructure assets. Another agency was centralizing decision-making authority in the office of the CIO for addressing troubled IT investments. In addition, one agency conducted a reorganization that placed component CIOs under the agency CIO. According to the CIO of that agency, the change has been a great asset to the organization, because it allowed the CIO office to work as a unit, created camaraderie among component CIOs, and reduced duplication of IT investments. In April 2011, the Federal CIO told us that agency CIOs should provide input to the component agency CIOs' performance review.

In addition to these agency-specific efforts, OMB has issued guidance to reaffirm and clarify the organizational, functional, and operational governance framework required within the executive branch for managing and optimizing the effective use of IT.<sup>69</sup> More recently, OMB has taken additional steps to increase the effectiveness of agency CIOs by clarifying their roles and authorities under the current law. For example, its 25 Point Implementation Plan to Reform Federal Information Technology Management called for agency CIOs to shift their focus from policy making and maintaining IT infrastructure to IT portfolio management. According to the plan, agency CIOs will be responsible for identifying unmet agency needs to be addressed by new projects, holding TechStat reviews, and improving or terminating poorly performing projects.

---

<sup>69</sup>OMB, *Memorandum for the Heads of Executive Departments and Agencies*, M-09-02 (Washington, D.C.: Oct. 21, 2008).

---

After we sent a draft of this report to agencies for comment, OMB issued a memorandum<sup>70</sup> outlining the primary areas of responsibility for federal agency CIOs. The guidance outlines four areas in which the CIO should have a lead role: IT governance, program management, commodity services, and information security. It emphasizes the role of the CIO in driving the investment review process and the CIO's responsibility over the entire IT portfolio for an agency. In a web log post about the memorandum, the Federal CIO stated that, next year, the administration will ask agencies to report through the President's Management Council<sup>71</sup> and the CIO Council on implementation of the memo.<sup>72</sup> In our view, the guidance is a positive step in reaffirming the importance of the role of CIOs in improving agency IT management.

Nonetheless, this guidance does not address the implementation weaknesses we have identified in this and our prior reviews—specifically that CIOs face significant limitations in their ability to influence IT investment decision making at their agencies and to exercise their statutory authority. The guidance generally instructs agency heads regarding the policies and priorities for CIOs in managing IT that we and others have stressed. However, the guidance does not state a specific requirement for agency heads to empower CIOs to carry out these responsibilities. Additionally, it does not require them to measure and report the progress of CIOs in carrying out these responsibilities and achieving the overall objectives of the IT Reform Plan. Such a requirement is essential to agencies empowering their CIOs to fully and effectively exercise their authority, and ultimately, ensuring that the CIOs are best positioned to be effective leaders in IT management. Without additional clarification and specific measures of accountability in OMB's guidance, agency CIOs are likely to continue to be hindered in carrying

---

<sup>70</sup>OMB, *Memorandum for Heads of Executive Departments and Agencies*, M-11-29 (Washington, D.C.: Aug. 8, 2011).

<sup>71</sup>The Council advises and assists the President in ensuring that government reform is implemented throughout the executive branch. The Council's functions include improving overall executive branch management; coordinating management-related efforts to improve government; ensuring the adoption of new management practices in agencies; and identifying examples of, and providing mechanisms for, interagency exchange of information about best management practices.

<sup>72</sup>OMB, Statement by Steven VanRoekel, Federal CIO, August 8, 2011, <http://www.whitehouse.gov/blog/2011/08/08/changing-role-federal-chief-information-officer>.

---

out their responsibilities and achieving successful outcomes in IT management, thus increasing the risk that IT spending will continue to produce mixed results, as we have long reported.

---

## A Structured Process Could Improve Sharing of Lessons Learned within Agencies

OMB guidance<sup>73</sup> requires and best practices suggest that agencies document lessons learned, and we have previously reported on the importance of their collection and dissemination.<sup>74</sup> The use of lessons learned is a principal component of an organizational culture committed to continuous improvement. Sharing such information serves to communicate acquired knowledge more effectively and to ensure that beneficial information is factored into planning, work processes, and activities. Lessons learned can be based on positive experiences or on negative experiences that result in undesirable outcomes. Documenting lessons learned can provide a powerful method of sharing successful ideas for improving work processes and increasing cost-effectiveness by aligning them to be utilized in the future.

To facilitate the sharing of best practices and lessons learned relating to IT management across the federal government, the CIO Council established the Management Best Practices Committee. The committee works to identify successful information technology best practices being implemented in industry, government, and academia and shares them with agency CIOs. As part of its mission, in April 2011, the committee launched a best practices information-sharing platform in the form of a website to which agencies can contribute case studies of best practices.

Federal agencies have begun to contribute by submitting examples depicting best practices relating to a range of topics including vendor communication and contract management; the consolidation of multiple systems into an enterprise solution through the use of cloud services; and program manager development. As of July 2011, the CIO Council website featured 10 case studies submitted by 10 agencies describing best practices. For example, one agency faced challenges with distributing technical support to 27 organizational units. After the agency head

---

<sup>73</sup>OMB Circular A-130 requires agencies to conduct postimplementation reviews to assess the project's impact on mission performance and document lessons learned.

<sup>74</sup>GAO, *NASA: Better Mechanisms Needed for Sharing Lessons Learned*, [GAO-02-195](#) (Washington, D.C.: Jan. 30, 2002).

---

directed the consolidation of IT support services under the CIO, the agency gained a better understanding of spending on services and equipment needed to provide IT support. In another example, an agency had been operating under separate e-mail systems, which prevented it from maximizing operational efficiency and productivity. Specifically, the agency faced high costs for maintaining individual systems; difficulty sending broadcast e-mails across the entire department, thus preventing the e-mails from being received in a timely fashion; difficulty obtaining accurate and complete contact information for all employees in one global address list; and difficulty operating calendar appointments. In order to address these challenges, the agency utilized a cloud-based service solution, which the agency explained would result in lower costs per user, an improved security posture, and a unified communication strategy.

In addition, agency CIOs told us their agency had implemented changes based upon lessons learned that have improved the effectiveness of the CIO. For example, while several CIOs implemented investment review boards or similar governance mechanisms, three CIOs explained that at their agency, senior-level officials, including deputy secretaries, and in one instance, an undersecretary, chaired these boards, which provided higher visibility over the selection, control, and evaluation of IT investments. Additionally, one CIO explained that implementing an enterprisewide licensing solution to optimize the agency's buying power resulted in a savings of \$200 million. One told us about improved effectiveness in information security through the use of a centralized information security center. Specifically, this CIO stated that all agency information went through this center, which provides real-time monitoring throughout agency systems. This CIO explained that the security center has helped to reduce the impact of intrusions to the agency's systems.

Nonetheless, although the CIO Council has established the management best practices committee and corresponding information-sharing platform to identify lessons learned, 19 CIOs said their agency did not have a process in place for capturing and documenting lessons learned and best practices. Two CIOs indicated that their agency did not have such a process due to a shortage of resources or because they did not see the development of such a process as being their responsibility. Without structured processes for capturing and documenting these lessons learned, agencies risk both losing the ability to share knowledge acquired with CIOs' experience and increasing the time required for newly hired CIOs to become effective. Additionally, the lack of internal documented processes for capturing lessons learned within agencies has the potential to inhibit the Management Best Practices Committee's ability to effectively

---

identify, document, and disseminate individual agencies' lessons learned and best practices throughout the federal government. By effectively identifying, documenting, and disseminating lessons learned internally and externally, agencies can mitigate risk and track successful ideas for improving work processes and cost-effectiveness that can be utilized in the future.

---

## Conclusions

As in 2004, federal agency CIOs currently are not consistently responsible for all of the 13 areas assigned by statute or identified as critical to effective IT management. While the majority of CIOs are primarily responsible for key IT management areas, they are less likely to have primary responsibility for information management duties. In this regard, CIOs spend two-thirds or more of their time in the IT management areas and attach greater importance to these areas compared with the information management areas.

Notwithstanding the focus on IT management, CIOs have not always been empowered to be successful. Despite the broad authority given to CIOs in federal law, these officials face limitations that hinder their ability to effectively exercise this authority, which has contributed to many of the long-standing IT management challenges we have found in our work. These limitations, which include control and influence over IT budgets, commodity IT investments, and staffing decisions, are consistent with issues we have previously identified that prevented CIOs from advising and influencing their agencies in managing IT for successful outcomes. While OMB's guidance reaffirms CIO authorities and responsibilities to influence IT outcomes, it does not establish measures of accountability. Having actionable measures would help ensure that CIOs are empowered to successfully carry out their responsibilities under the law and enable them to successfully carry out their responsibilities under the IT Reform Plan.

Finally, while agency CIOs told us they had implemented practices they believed have improved the management of IT, they had not established processes to document agency-specific lessons learned that could be shared within the agency. Not doing so increases the likelihood of new CIOs making the same mistakes as those they are replacing, while establishing such a mechanism could better enable succession planning and knowledge transfer between CIOs.



---

## Recommendations for Executive Action

To ensure that CIOs are better able to carry out their statutory role as key leaders in managing IT, we recommend the Director of OMB take the following three actions:

- Issue guidance to agencies requiring that CIOs' authorities and responsibilities, as defined by law and by OMB, are fully implemented, taking into account the issues raised in this report.
- Establish deadlines and metrics that require agencies to demonstrate the extent to which their CIOs are exercising the authorities and responsibilities provided by law and OMB's guidance.
- Require agencies to identify and document internal lessons learned and best practices for managing information technology.

---

## Agency Comments and Our Evaluation

We received comments on a draft of this report from OMB and from 5 of the 30 agencies included in our study. In oral comments, OMB's Deputy Administrator for e-Gov and its Policy Analyst for e-Gov, within the Office of Electronic Government and Information Technology, generally agreed with our findings and stated that the agency had taken actions that addressed our recommendations. Specifically, with regard to our first recommendation, the officials said they believed OMB's August 8, 2011, memorandum discussing CIOs' authorities aligned with, and reflected the beginning of a process that would help address, the concerns noted in our report. Thus, they believed our recommendation had been addressed with OMB's issuance of the memorandum. With regard to our second recommendation that called for OMB to establish an appropriate reporting mechanism to ensure compliance with the guidance, the officials pointed to a recent web log post about the August memorandum. In the post, the Federal CIO stated that, in 2012, the administration will ask agencies to report through the President's Management Council and the CIO Council on implementation of the memorandum.

We believe the guidance reflected in OMB's August 2011 memorandum is a positive step in reaffirming the importance of the role of CIOs in improving agency IT management and toward addressing the concerns that are the basis for our first recommendation. It highlights the responsibilities of CIOs in the four areas of IT governance, program management, commodity services, and information security. These responsibilities are consistent with requirements in law and best practices. Further, OMB's planned use of the councils for agency reporting on implementation of the memorandum could be a useful

---

mechanism for helping to ensure CIOs' accountability for effectively managing IT.

However, neither the guidance nor the planned use of the councils, as referenced, identify requirements that would hold agencies accountable for ensuring effective CIO leadership in the four IT management areas. Specifically, as pointed out earlier in this report, the guidance does not articulate a requirement for agencies to measure and report the progress of CIOs in carrying out their responsibilities and authorities. Such a requirement is essential to ensuring that agency CIOs are best positioned to be effective leaders in IT management. As such, we stand by our second recommendation but have revised it to more explicitly highlight the need for OMB to establish deadlines and metrics that require agencies to demonstrate the extent to which CIOs are exercising their authorities and responsibilities.

With regard to our third recommendation, that OMB require agencies to establish processes for documenting internal lessons learned and best practices, the officials believed this recommendation was addressed by existing guidance<sup>75</sup> requiring agencies to document lessons learned for post-implementation reviews of IT projects. However, as discussed earlier, most of the agencies in our study reported that they had not established processes for documenting internal lessons learned. Further, the guidance to which OMB's officials referred is limited to lessons learned for post-implementation reviews of specific IT projects and does not include the broader spectrum of IT management areas, such as program management and information security. As such, we continue to believe that agencies could benefit from having established internal processes for documenting lessons learned across the broader spectrum of IT management areas and, therefore, believe our recommendation is warranted.

Although we made no specific recommendations to the 30 agencies included in our review, we sent each agency a draft of the report for comment. Twenty-five of the agencies told us they had no comments on the draft report, while five agencies provided e-mail or written comments on the report, as follows.

---

<sup>75</sup>OMB, Circular No. A-130 (Washington, D.C.: Nov. 28, 2000).

- 
- 
- In written comments from the Department of Defense CIO, the department concurred with our recommendations to OMB. However, the CIO also stated that, while our report did not identify legislative changes needed to enhance current CIOs' authority and generally felt that existing law provides sufficient authority, the department believes there are legislative opportunities to clarify and strengthen CIO authorities that should be pursued, such as overlap in responsibilities between the CIO and other officials. The department stated that it was taking actions to address this issue internally. As discussed earlier in this report, the effectiveness of agency CIOs depends in large measure on their having clear roles and authorities. As noted, however, we found no evidence indicating that legislative changes are needed to achieve this. Rather, our study results determined that these officials face limitations that hinder their ability to effectively exercise their current authorities. Accordingly, agencies have an important opportunity to address these limitations by empowering the CIOs to fully and effectively exercise their authority and ensuring that the CIOs are best positioned to be effective leaders in managing IT. Our recommendations to OMB are aimed at ensuring that CIOs effectively exercise the authority and responsibilities that they have been given. DOD's comments are reprinted in appendix VI.
  - The Department of Homeland Security's Director of Departmental GAO/Office of Inspector General (OIG) Liaison Office provided written comments in which the department indicated agreement with our findings and recommendations. In the comments, the department said it is committed to working with OMB to address the challenges agency CIOs face and increase the effectiveness of its efforts. These comments are reproduced in appendix VII.
  - In written comments from the CIO, the Office of Personnel Management agreed with our recommendations. The agency included examples of actions the agency has taken to elevate the CIO position and bring it into greater alignment with the Clinger-Cohen Act. The Office of Personnel Management's written comments are reproduced in appendix VIII.
  - In an e-mail response from the Office of the Chief Information Officer, the United States Agency for International Development said the recommendations were sound and would assist agencies in ensuring that CIOs are better able to carry out their statutory role as key leaders in managing IT.
  - In an e-mail response from the Deputy CIO, the Department of Commerce stated that it had no major issues with the

---

recommendations and conclusions and described the report as an informative assessment of the practices and challenges faced by federal agency CIOs.

Beyond the aforementioned comments, two agencies—the Social Security Administration and the Department of Health and Human Services—provided technical comments on the report, which we incorporated as appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to other interested congressional committees, the Director of the Office of Management and Budget, and the Secretaries of Agriculture, the Air Force, the Army, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Labor, the Navy, State, Transportation, the Treasury, and Veterans Affairs; the Attorney General; the administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Small Business Administration, and U.S. Agency for International Development; the commissioners of the Nuclear Regulatory Commission and the Social Security Administration; the directors of the National Science Foundation and Office of Personnel Management; the Chief Executive Officer of the Corporation for National and Community Service; and the chairmen of the Federal Labor Relations Authority and Commodity Futures Trading Commission. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-6304 or by e-mail at [melvinv@gao.gov](mailto:melvinv@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs are on the last page of this report. Key contributors to this report are listed in appendix IX.

*Valerie C. Melvin*

Valerie C. Melvin  
Director,  
Information Management and Human Capital Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to (1) determine the current roles and responsibilities of federal agency Chief Information Officers (CIO) in managing information and technology; (2) determine what potential modifications to the Clinger-Cohen Act and related laws could be made to enhance CIOs' authority and effectiveness; and (3) identify key lessons learned by federal agency CIOs in managing information and technology.

To address the objectives of this review, we collected and reviewed previous GAO reports, including our 2004 report on CIOs' roles and responsibilities,<sup>1</sup> as well as various other reports that discussed the status of agency CIOs' roles and responsibilities. This included reports from Gartner<sup>2</sup> and Deloitte<sup>3</sup> on the role of federal CIOs and OMB's 25 Point Implementation Plan to Reform Federal Information Technology Management.<sup>4</sup> We also interviewed the Partnership for Public Service's Director of the Strategic Advisors to Government Executives Program for mentoring federal executives, including agency CIOs.

We then developed and administered a questionnaire to the CIOs of 27 major departments and agencies in our 2004 review and of three small, independent agencies. We selected the three independent agencies based on whether they had a CIO in place when our review began and the size of the agency's 2011 budget estimates.<sup>5</sup> Using the questionnaire, we requested information on whether each CIO was responsible for each of 13 information technology (IT) and information management areas that we identified as either required by statute or critical to effective IT management in our 2004 report.<sup>6</sup> In addition, we asked about CIOs'

---

<sup>1</sup>GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, [GAO-04-823](#) (Washington, D.C.: July 21, 2004).

<sup>2</sup>Gartner, *The Role of Federal Government CIOs Must Evolve*, ID Number: G00130848 (Sept. 28, 2005); *2011 Predicts: Government CIOs Must Balance Cost Containment With IT Innovation*, ID Number: G00208687 (Nov. 17, 2010); and *Private-Turned-Public CIOs Must Acquire Different Political and Interpersonal Skills*, ID Number G00127518 (July 1, 2005).

<sup>3</sup>Deloitte, *CIO 2.0: The Changing Role of the CIO in Government* (2004); and *Top Ten Challenges for CIOs in 2010: Tough Growth, Tough Decisions* (2010).

<sup>4</sup>OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

<sup>5</sup>We selected agencies to represent a range of 2011 IT budget estimates of approximately \$25 million to \$860 million.

<sup>6</sup>[GAO-04-823](#).

reporting relationships, professional and educational backgrounds, tenure, and lessons learned in managing information and technology.

In addition, we collected and reviewed written position descriptions for each agency's CIO, deputy CIO, and other key officials responsible for the 13 IT and information management areas; the resumes or curricula vitae of the current CIOs; each agency's current organization chart(s) depicting the CIO's position relative to the head of the agency, other senior officials, and component CIOs, if applicable; and functional statements for offices that have responsibilities in IT and information management. We also asked each agency to supply the name, beginning and ending dates in office, and circumstances (e.g., whether they were in an acting or permanent position) of each of the individuals who had served as CIO at the agency since 2003. Further, we also collected and reviewed any supporting documentation of recent departmental changes.

We then interviewed each of the CIOs who were in place at the time of our review (see app. II for a list of the CIOs) in order to validate responses from the questionnaire and to obtain an understanding of their views on the 13 IT and information management areas including roles and responsibilities, changes needed to enhance authority and effectiveness, and lessons learned for managing information and technology.

From the questionnaire and interview responses, we analyzed CIOs' responses to determine their current roles and responsibilities and reporting relationships with agency heads. We then compared the responses to those identified in our 2004 report.<sup>7</sup> Additionally, we assessed the CIOs' reported time spent in the 13 IT and information management areas of responsibility and the importance of each area to them, as well as their views on changes needed to improve their authority and effectiveness. We also reviewed CIOs' qualifications and current and former CIOs' tenure. Further, we analyzed CIO responses to questions concerning changes needed to improve their authority and effectiveness and compared them to the authority described in federal IT laws. We supplemented our analysis by reviewing our prior reports related to

---

<sup>7</sup>When comparing results between this report and our 2004 review, we did not include information from the three small, independent agencies, as they were not involved in our 2004 review.

agency CIO authority and IT management challenges.<sup>8</sup> We also analyzed CIOs' comments related to lessons learned that they have used to improve IT management at their agency. Further, we analyzed OMB IT management reform efforts, including its August 2011 memorandum on CIO authorities, and status updates related to agency CIOs and lessons learned initiatives.

To complement information we obtained from current CIOs, we held a panel discussion with nine former CIOs of federal agencies. The purpose of this discussion was to elicit views regarding the statutory responsibilities given to federal CIOs, lessons learned by CIOs in managing information and technology, and areas in which current legislation could be revised to enhance CIOs' authority and effectiveness. Appendix III lists these panelists. Finally, we met with the Federal CIO to obtain his views on priorities and responsibilities for CIOs and to discuss potential modifications to the Clinger-Cohen Act and related laws that could enhance CIOs' authority and effectiveness.

We conducted our work at the 30 agencies from June 2010 to September 2011 in the greater Washington, D.C., area, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

<sup>8</sup>GAO, *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, [GAO-04-509](#) (Washington, D.C.: May 21, 2004); *Information Technology: HHS Has Several Investment Management Capabilities in Place but Needs to Address Key Weaknesses*, [GAO-06-11](#) (Washington, D.C.: Oct. 28, 2005); *DOD Business Transformation: Improved Management Oversight of Business Systems Modernization Efforts Needed*, [GAO-11-53](#) (Washington, D.C.: Oct. 7, 2010); and [GAO-04-823](#).

# Appendix II: Chief Information Officers Interviewed

<b>Agency/department</b>	<b>CIO</b>
Commodity Futures Trading Commission (CFTC)	John Rogers
Corporation For National and Community Service (CNCS)	Phillip Clark
Department of Agriculture	Christopher Smith
Department of Commerce	Simon Szykman
Department of Defense	Teresa M. Takai
Department of the Air Force	Lieutenant General William T. Lord
Department of the Army	Michael E. Krieger <sup>a</sup>
Department of the Navy	Terry Halverson
Department of Education	Danny Harris
Department of Energy	Michael W. Locatis III
Department of Health and Human Services (HHS)	Michael W. Carleton
Department of Homeland Security (DHS)	Richard Spires
Department of Housing and Urban Development (HUD)	Jerry E. Williams
Department of the Interior	Bernard Mazer
Department of Justice	Vance Hitch
Department of Labor	T. Michael Kerr
Department of State	Susan Swart
Department of Transportation (DOT)	Nitin Pradhan
Department of the Treasury	Diane Litman <sup>a</sup>
Department of Veterans Affairs (VA)	Roger W. Baker
Environmental Protection Agency (EPA)	Malcolm D. Jackson
Federal Labor Relations Authority (FLRA)	Chris Webber
General Services Administration (GSA)	Casey Coleman
National Aeronautics and Space Administration (NASA)	Linda Y. Cureton
National Science Foundation (NSF)	Andrea T. Norris
Nuclear Regulatory Commission (NRC)	Darren B. Ash
Office of Personnel Management (OPM)	Matthew Perry
Small Business Administration (SBA)	Paul Christy
Social Security Administration (SSA)	Franklin Baitman
U.S. Agency for International Development (USAID)	Jerry Horton

Source: GAO

<sup>a</sup>These CIOs were in their position during the time of our review, but left their position prior to the end of our review.



# Appendix III: Former Agency CIO Panel Participants

In March 2011, we convened a panel of former federal agency chief information officers, during which we discussed CIOs' roles and responsibilities, reporting relationships, and any potential changes needed to legislation. Table 5 provides the former and current titles of these officials.

**Table 5: Former Agency Chief Information Officer Panel**

<b>Name</b>	<b>Former agency/positions</b>	<b>Current organization/position</b>
Alan Balutis	Department of Commerce/CIO	Cisco Systems' Business Solutions Group/Senior Director of North American Public Sector
John Gilligan	Department of the Air Force/CIO; Department of Energy/CIO	The Gilligan Group/President
Thomas Hughes	Social Security Administration/CIO	CSC Corporation/Partner in Strategy Services
Daniel Matthews	Department of Transportation/CIO	Triple-I Corporation/Senior Vice President of Strategic Programs
Molly O'Neil	U.S. Environmental Protection Agency/CIO	CGI Group/VP Consulting
Gloria Parker	Department of Housing and Urban Development/CIO; Department of Education/ Deputy CIO	Parker Group Consulting/CEO and Senior Partner
Patrick Pizzella	Department of Labor/ Assistant Secretary for Administration and Management and CIO	Patrick Pizzella, LLC
W. Hord Tipton	Department of the Interior/CIO	International Information Systems Security Certification Consortium (ISC)/Executive Director and member of the Board of Directors
Barry West	Department of Commerce/CIO; Federal Emergency Management Agency/CIO	SE Solutions/Executive Vice President

Source: GAO.

# Appendix IV: Summary of CIOs' Information Management and Technology Responsibilities

The following summarizes information gathered from CIOs related to their responsibilities in the 13 information management and information technology management areas discussed in this report.

## IT Strategic Planning

CIOs are responsible for strategic planning for all information and information technology management functions [Paperwork Reduction Act].

Of the 30 CIOs we surveyed, all CIOs indicated they were responsible for ensuring compliance with laws related to IT strategic planning within their agency. In 2004, all 27 CIOs surveyed also indicated responsibility for IT strategic planning.

All CIOs reported they thought the CIO should be responsible for IT strategic planning. Twenty-nine of the 30 CIOs reported that IT strategic planning was important to carrying out their mission. The CIO who reported that IT strategic planning was not important said this area was being executed properly and it did not require much attention or guidance. Table 6 provides a summary of CIO responses regarding IT strategic planning.

**Table 6: Summary of CIO Responses to Questions for IT Strategic Planning**

<b>CIOs responsible for IT strategic planning</b>	<b>Percentage</b>
2011 - CIOs responsible	100%
2004 - CIOs responsible	100
CIOs who felt they should be responsible	100
CIOs who felt they should not be responsible	0
<b>Importance of IT strategic planning</b>	
Very important	83
Important	13
Somewhat important	0
Not very important	3
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

**IT Workforce Planning**

CIOs are responsible for assessing agency information and IT workforce needs and developing strategies and plans for meeting those needs [Paperwork Reduction Act and Clinger-Cohen Act].

Twenty-six of the 30 CIOs indicated they were responsible for strategically assessing IT workforce needs and using IT staff in order to achieve mission goals in the most efficient ways. In 2004, we reported that all 27 CIOs responded they were responsible for helping the agency meet its IT workforce or human capital needs.

Of the 30 CIOs that provided responses, 24 reported that they thought the CIO should be responsible by law for IT workforce planning. All of the 30 CIOs reported that workforce planning was “very important” or “important” to carrying out their mission. Table 7 provides a summary of CIO responses regarding IT workforce planning.

**Table 7: Summary of CIO Responses to Questions for IT Workforce Planning**

<b>CIOs responsible for IT workforce planning</b>	<b>Percentage</b>
2011 - CIOs responsible	87%
2004 - CIOs responsible	100
CIOs who felt they should be responsible	80
CIOs who felt they should not be responsible	20
<b>Importance of IT workforce planning</b>	
Very important	63
Important	37
Somewhat important	0
Not very important	0
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

**Capital Planning and Investment Management**

CIOs are responsible for a process for selecting, controlling, and evaluating IT investments to produce business value, reduce investment-related risks, and increase accountability and transparency in the investment decision-making process [Paperwork Reduction Act and Clinger-Cohen Act].

Of the 30 CIOs we surveyed, all of them indicated they were responsible for capital planning and investment management activities at their agency. This is consistent with the results of our 2004 report, which found that all 27 CIOs also indicated responsibility for capital planning and investment management.

All 30 of the CIOs reported they thought the CIO should be responsible for capital planning and investment management. All 30 CIOs reported that capital planning and investment management was "very important" or "important" to carrying out their mission. Table 8 provides a summary of CIO responses regarding capital planning and investment management.

**Table 8: Summary of CIO Responses to Questions for Capital Planning and Investment Management**

CIOs responsible for capital planning and investment management	Percentage
2011 - CIOs responsible	100%
2004 - CIOs responsible	100
CIOs who felt they should be responsible	100
CIOs who felt they should not be responsible	0
<b>Importance of capital planning and investment management</b>	
Very important	97
Important	3
Somewhat important	0
Not very important	0
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Information Security

CIOs are responsible for ensuring agency compliance with requirements to protect information and systems [Paperwork Reduction Act, Federal Information Security Management Act, and Clinger-Cohen Act].

All 30 CIOs indicated they were responsible for ensuring compliance with information security best practices and related laws at their agency. This is consistent with the results of our 2004 report, which found that all of the 27 CIOs surveyed indicated being responsible for information security.

Of the 30 agencies that provided responses, all 30 CIOs reported that they thought the CIO should be responsible by law for information

security. Twenty-nine of the 30 CIOs reported that information security was “very important” to carrying out their mission. Only one CIO ranked information security as “somewhat important” because his goal is to move the agency toward a risk-based approach that uses secure, reliable, and cost-effective technology. Table 9 provides a summary of CIO responses regarding information security.

**Table 9: Summary of CIO Responses to Questions for Information Security**

<b>CIOs responsible for information security</b>	<b>Percentage</b>
2011 - CIOs responsible	100%
2004 - CIOs responsible	100
CIOs who felt they should be responsible	100
CIOs who felt they should not be responsible	0
<b>Importance of information security</b>	
Very important	97
Important	0
Somewhat important	3
Not very important	0
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Enterprise Architecture

CIOs are responsible for developing and maintaining the business and technology blueprint that links an agency’s strategic plan to IT programs and supporting system implementations [Clinger-Cohen Act].

Of the 30 CIOs we surveyed, all 30 indicated they were responsible for enterprise architecture-related activities at their agency. This is consistent with the results of our 2004 report, which found that 27 of 27 CIOs also indicated responsibility for enterprise architecture.

All 30 CIOs interviewed reported that they believed the CIO should be responsible for enterprise architecture. Twenty-eight of the 30 CIOs reported that enterprise architecture was “important” or “very important” to carrying out their mission with one of the remaining two identifying it as being “somewhat important” and the other labeling it as being “not very important.” For example, one CIO ranked enterprise architecture as being very important based on the maturity of the agency’s abilities within the

area. The CIO explained that, since their enterprise architecture was not as mature as they would like it to be, they viewed it as being currently very important. The CIO who reported that enterprise architecture was somewhat important for his mission clarified that this was because the existing activities related to enterprise architecture were being properly executed and therefore required less focus. The remaining CIO who responded that enterprise architecture was “not very important” explained that enterprise architecture was not essential to completing the agency’s mission and therefore having a formal enterprise architecture was less important at the agency. Table 10 provides a summary of CIO responses regarding enterprise architecture.

**Table 10: Summary of CIO Responses to Questions for Enterprise Architecture**

<b>CIOs responsible for enterprise architecture</b>	<b>Percentage</b>
2011 - CIOs responsible	100%
2004 - CIOs responsible	100
CIOs who felt they should be responsible	100
CIOs who felt they should not be responsible	0
<b>Importance of enterprise architecture</b>	
Very important	77
Important	17
Somewhat important	3
Not very important	3
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire

Note: Percentages may not sum to 100 due to rounding.

**Systems Acquisition, Development, and Integration**

CIO IT management responsibilities should include a primary role in developing and enforcing policies for systems acquisition, their development, and integration with existing systems [Paperwork Reduction Act and Clinger-Cohen Act].

Of the 30 CIOs we surveyed, 27 indicated they were responsible for ensuring compliance with systems acquisitions, development, and integration-related best practices. This is generally consistent with our 2004 study, when 25 of 27 CIOs reported responsibility for systems acquisition, development, and integration.

Almost all (28 of 30) CIOs reported that they thought the CIO should be responsible for systems acquisition, development, and integration. All of the 30 CIOs reported that systems acquisition, development, and integration was “very important” or “important” to carrying out their mission. Table 11 provides a summary of CIO responses regarding this area.

**Table 11: Summary of CIO Responses to Questions for Systems Acquisition, Development, and Integration**

<b>CIOs responsible for systems acquisition, development, and integration</b>	<b>Percentage</b>
2011 - CIOs responsible	90%
2004 - CIOs responsible	93
CIOs who felt they should be responsible	93
CIOs who felt they should not be responsible	7
<b>Importance of systems acquisition, development, and integration</b>	
Very important	77
Important	23
Somewhat important	0
Not very important	0
Not at all important	0
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## E-government Initiatives

CIOs are responsible for promoting the use of IT, including the Internet and emerging technologies, to improve the productivity, efficiency, and effectiveness of agency operations, programs, and services [Paperwork Reduction Act, Clinger-Cohen Act, and E-Government Act of 2002].

Of the 30 CIOs we surveyed, 28 indicated they were responsible for ensuring compliance with the E-government Act of 2002 and related e-government initiatives at their agency. This is generally consistent with the results of our 2004 report, which found that 25 of 27 CIOs indicated responsibility for the e-government initiatives.

Twenty-six of 30 CIOs reported that they thought the CIO should be responsible for e-government initiatives. Eighteen of the 30 CIOs reported that the e-government initiatives were “important” or “very important” to carrying out their mission. However, a number of CIOs felt that the e-

government initiatives were not important to their mission. For example, one CIO said the only persons who cared whether they respond to the e-government initiatives are outside of the agency and this CIO considered these initiatives a paperwork exercise. Another CIO felt this area was only "somewhat important" because they already had established mature systems that did not require effort on the CIOs part to maintain. Table 12 provides a summary of CIO responses regarding e-government.

**Table 12: Summary of CIO Responses to Questions for E-government Initiatives**

<b>CIOs responsible for e-government initiatives</b>	<b>Percentage</b>
2011 - CIOs responsible	93%
2004 - CIOs responsible	93
CIOs who felt they should be responsible	87
CIOs who felt they should not be responsible	13
<b>Importance of e-government initiatives</b>	
Very important	23
Important	37
Somewhat important	23
Not very important	10
Not at all important	7
N/A	0

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

**Information Collection/Paperwork Reduction**

CIOs are responsible for the review of agency information collection proposals to maximize utility and minimize public paperwork burdens [Paperwork Reduction Act].

Twenty-two of 30 CIOs indicated that they were responsible for information collection/paperwork reduction at their agency. This is generally consistent with the results of our 2004 study, which found that 22 of 27 CIOs indicated responsibility for information collection/paperwork reduction.

Eighteen of the 30 CIOs reported they thought the CIO should be responsible for information collection/paperwork reduction. Fourteen of the 30 CIOs reported that information collection/paperwork reduction was "very important" or "important" to carrying out their mission. Fifteen CIOs ranked it as "somewhat important" or "not very important." Four CIOs



reported that information collection/paperwork reduction was “not very important,” with one stating that this area was either handled by his staff or he felt it was being executed properly and did not require a lot of attention and guidance. Several of the remaining CIOs reported that information collection/paperwork reduction was “somewhat important” because they were either not responsible for this area or it was not mission critical. Table 13 provides a summary of CIO responses regarding this area.

**Table 13: Summary of CIO Responses to Questions for Information Collection/Paperwork Reduction**

<b>CIOs responsible for information collection/paperwork reduction</b>	<b>Percentage</b>
2011 - CIOs responsible	73%
2004 - CIOs responsible	81
CIOs who felt they should be responsible	60
CIOs who felt they should not be responsible	40
<b>Importance of information collection/paperwork reduction</b>	
Very important	17
Important	30
Somewhat important	37
Not very important	13
Not at all important	0
N/A	3

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Information Dissemination

CIOs are responsible for ensuring that the agency’s information dissemination activities meet policy goals, such as timely and equitable public access to information [Paperwork Reduction Act].

Of the 30 CIOs we surveyed, 16 indicated they were responsible for information dissemination-related activities at their agency. This represents a decrease since our 2004 report when 20 of 27 CIOs reported they held this responsibility.

Thirteen of the 30 CIOs reported that they thought the CIO should be responsible for information dissemination. Eighteen of the 30 CIOs reported that information dissemination was “very important” or “important” to carrying out their mission, while 11 CIOs ranked it as being either “somewhat important” or “not very important” to carrying out their

mission. Several CIOs explained they ranked information dissemination as being less than “important” because responsibilities in the area were being executed properly by other designated officials, they were not directly responsible, or it was not a priority and did not require a lot of time. Table 14 provides a summary of CIO responses regarding information dissemination.

**Table 14: Summary of CIO Responses to Questions for Information Dissemination**

<b>CIOs responsible for information dissemination</b>	<b>Percentage</b>
2011 - CIOs responsible	53%
2004 - CIOs responsible	74
CIOs who felt they should be responsible	43
CIOs who felt they should not be responsible	57
<b>Importance of information dissemination</b>	
Very important	17
Important	43
Somewhat important	30
Not very important	7
Not at all important	0
N/A	3

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Information Disclosure

CIOs are responsible for ensuring appropriate information disclosure under the Freedom of Information Act [Paperwork Reduction Act].

Of the 30 CIOs we surveyed, 9 indicated that they were responsible for information disclosure at their agency. This is generally consistent with our 2004 findings in which 9 of 27 CIOs indicated responsibility for information disclosure.

Of the 30 CIOs surveyed, 10 reported that they thought the CIO should be responsible for information disclosure. Fourteen of the 30 CIOs reported that it was “very important” or “important” to carrying out their mission. In contrast, 14 of the 30 CIOs reported that information disclosure was either “somewhat important” or “not very important” to carrying out their mission. CIOs who ranked information disclosure as either being “somewhat important” or “not very important” commonly explained they did so because the area was either a low priority, did not require a lot of time, was executed properly or, as CIO, they were not

primarily responsible for information disclosure. One CIO explained that he ranked the area as being “somewhat important” because his agency does not disclose a majority of its information. Of the remaining 2 CIOs who responded that this question was not applicable, one explained that they ranked the area as “not applicable” because they were not directly responsible and felt uncomfortable providing a metric regarding its importance. Table 15 provides a summary of CIO responses regarding information disclosure.

**Table 15: Summary of CIO Responses to Questions for Information Disclosure**

<b>CIOs responsible for information disclosure</b>	<b>Percentage</b>
2011 - CIOs responsible	30%
2004 - CIOs responsible	33
CIOs who felt they should be responsible	33
CIOs who felt they should not be responsible	67
<b>Importance of information disclosure</b>	
Very important	17
Important	30
Somewhat important	37
Not very important	10
Not at all important	0
N/A	7

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Statistical Policy and Coordination

CIOs are responsible for agency statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes [Paperwork Reduction Act].

Seven of 30 CIOs indicated they had responsibility for performing statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes at their agency. Similarly, in our 2004 study, 8 of 27 CIOs reported responsibility for statistical policy and coordination.

Twenty-three CIOs reported that someone other than the CIO should be responsible for statistical policy and coordination. In comparison to the other areas of information and IT management, CIOs viewed statistical

policy and coordination as the least important to accomplishing the CIO's mission. Specifically, 15 CIOs ranked statistical policy as "somewhat important," "not very important," or "not at all important." Many of these CIOs explained that they were not responsible for statistical policy at the agency because a designated official performed these activities. Table 16 provides a summary of CIO responses regarding statistical policy and coordination.

**Table 16: Summary of CIO Responses to Questions for Statistical Policy and Coordination**

<b>CIOs responsible for statistical policy and coordination</b>	<b>Percentage</b>
2011 - CIOs responsible	23%
2004 - CIOs responsible	30
CIOs who felt they should be responsible	20
CIOs who felt they should not be responsible	80
<b>Importance of statistical policy and coordination</b>	
Very important	13
Important	13
Somewhat important	23
Not very important	20
Not at all important	6
N/A	23

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Records Management

CIOs are responsible for ensuring that the agency implements and enforces the records management policies and procedures required by the Federal Records Act [Paperwork Reduction Act].

Of the 30 CIOs we surveyed, 18 indicated they were responsible for ensuring compliance with the Federal Records Act and related laws at their agency. In our 2004 study, 21 of 27 CIOs indicated responsibility for records management.

Of the 30 CIOs surveyed, 18 reported that they thought the CIO should be responsible for records management. Twenty-one of the 30 CIOs reported that records management was "important" or "very important" to carrying out their mission. However, 8 CIOs felt that records management was "somewhat important" or "not very important" to their mission. Of these, one CIO said this area was either handled by his staff or he felt it

was being executed properly and did not require a lot of attention or guidance. Another CIO felt this area was “somewhat important” because it did not have a lot of impact and was of minimal importance. Table 17 provides a summary of CIO responses regarding records management.

**Table 17: Summary of CIO Responses to Questions for Records Management**

<b>CIOs responsible for records management</b>	<b>Percentage</b>
2011 - CIOs responsible	60%
2004 - CIOs responsible	78
CIOs who felt they should be responsible	60
CIOs who felt they should not be responsible	40
<b>Importance of records management</b>	
Very important	27
Important	43
Somewhat important	23
Not very important	3
Not at all important	0
N/A	3

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

## Privacy

CIOs are responsible for ensuring agency compliance with the Privacy Act and related laws [Paperwork Reduction Act].

Eighteen of 30 CIOs indicated they were responsible for ensuring compliance with the Privacy Act and related laws at their agency. In our 2004 study, 17 of 27 CIOs were responsible for privacy.

Seventeen CIOs reported that they thought the CIO should be responsible for privacy. Twenty-nine of the 30 CIOs reported that privacy was “important” or “very important” to carrying out their mission. The CIO who reported that this question was not applicable clarified that because he was not responsible for privacy, he was not comfortable assessing its importance. Table 18 provides a summary of CIO responses regarding privacy.

**Table 18: Summary of CIO Responses to Questions for Privacy**

<b>CIOs responsible for privacy</b>	<b>Percentage</b>
2011 - CIOs responsible	60%
2004 - CIOs responsible	63
CIOs who felt they should be responsible	57
CIOs who felt they should not be responsible	43
<b>Importance of privacy</b>	
Very important	60
Important	37
Somewhat important	0
Not very important	0
Not at all important	0
N/A	3

Source: CIO responses to GAO questionnaire.

Note: Percentages may not sum to 100 due to rounding.

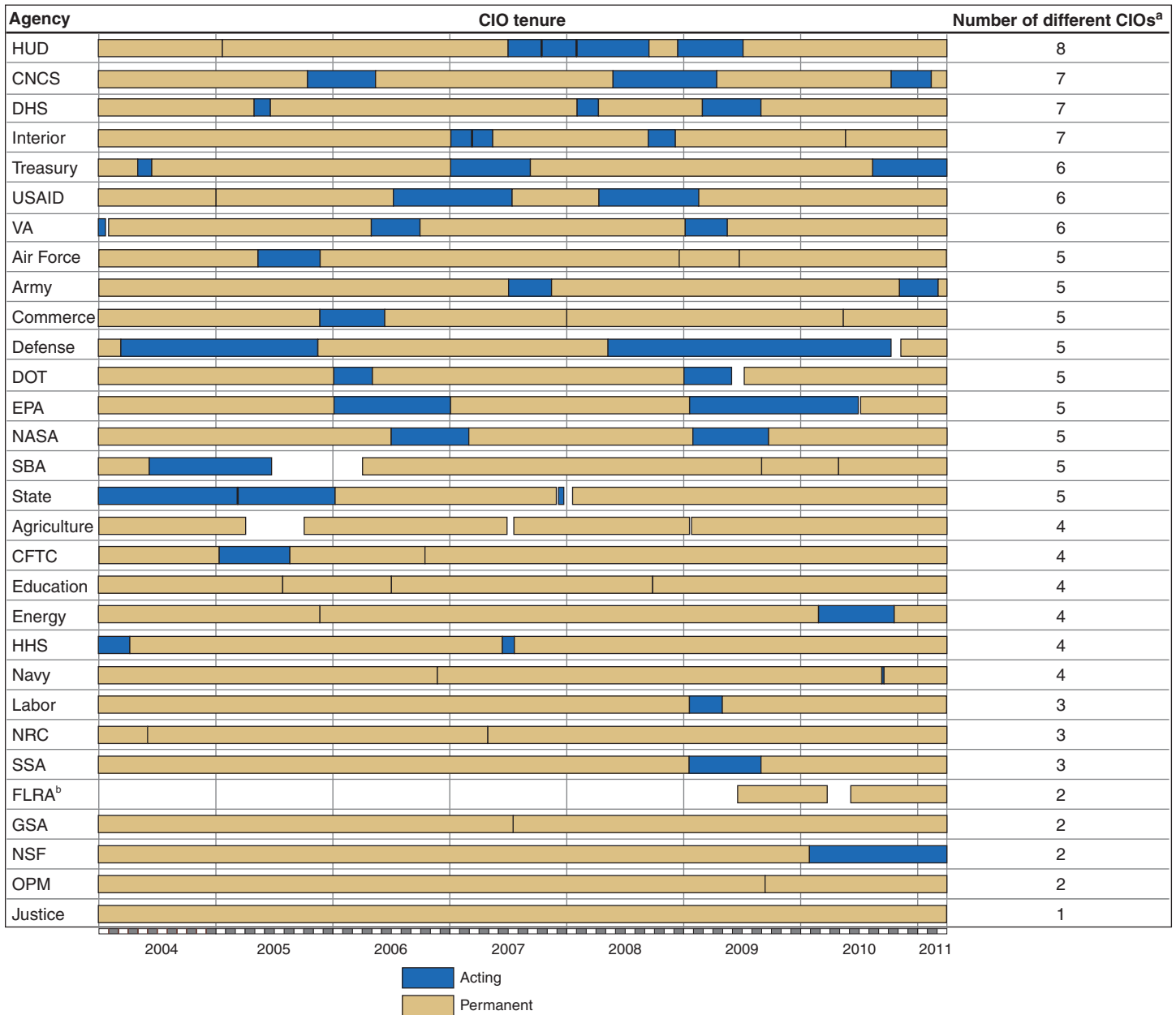
---

# Appendix V: CIO Tenure at Each Agency

---

Figures 2 and 3 depict the tenure of CIOs at each agency in our review from 2004 to 2011. In addition, figure 2 shows whether CIOs were acting or permanent, while figure 3 shows whether they were career employees or political appointees. Table 19 presents further analysis related to acting and permanent CIO tenure.

Figure 2: CIO Tenure—Acting and Permanent



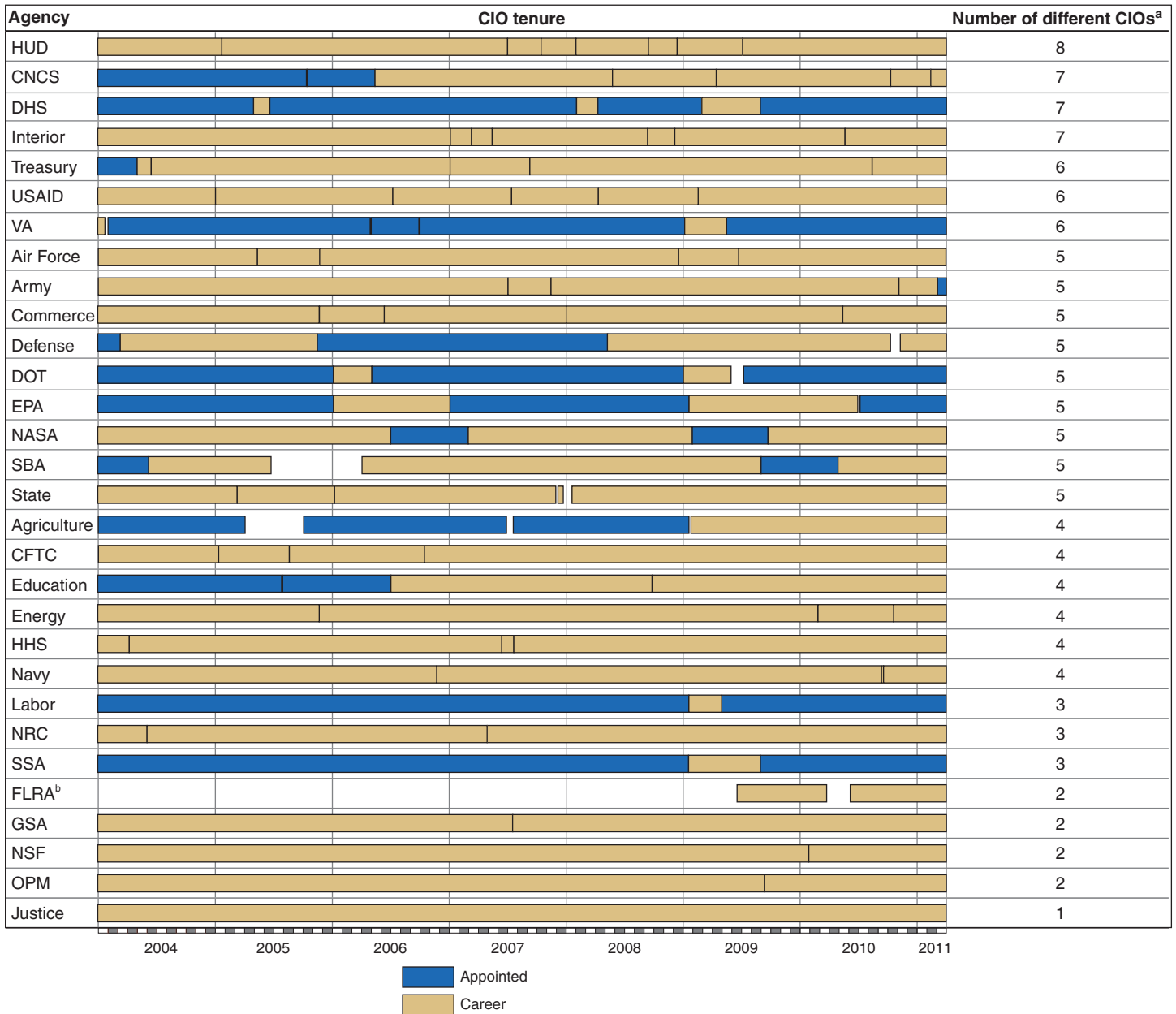
Source: GAO analysis of agency data.

<sup>a</sup>The number of bar elements for an agency may not add up to the total in this column because some individual CIOs are shown more than once, as their circumstances changed (e.g., an acting CIO that became a permanent CIO).

<sup>b</sup>FLRA did not have a CIO until 2009. It is one of the independent agencies that was not required to have a CIO under the Clinger-Cohen Act.



Figure 3: CIO Tenure—Career and Political Appointees



Source: GAO analysis of agency data.

<sup>a</sup>The number of bar elements for an agency may not add up to the total in this column because some individual CIOs are shown more than once, as their circumstances changed (e.g., an acting CIO that became a permanent CIO).

<sup>b</sup>FLRA did not have a CIO until 2009. It is one of the independent agencies that was not required to have a CIO under the Clinger-Cohen Act.

**Table 19: Statistical Analysis of CIO Tenure (2004-2011)**

	Permanent and acting CIOs including current CIOs	Permanent and acting CIOs excluding current CIOs	Permanent CIOs including current CIOs	Permanent CIOs excluding current CIOs	Acting CIOs including current CIOs	Acting CIOs excluding current CIOs	Only current permanent CIOs
Mean	23	23	31	33	9	9	25
Median	18	17	27	30	7	7	21
Minimum(in months)	0.3	0.3	2	3	0	0	2
Maximum (in months)	160	160	160	160	74	74	109
Number of CIOs in this population	134	104	86	60	44	41	26
Number of CIOs in office less than 3 years	107	83	60	40	43	40	20
Number of CIOs in office between 3 and 5 years	20	15	20	15	0	0	5
Percentage of CIOs in office greater than 5 years	7	6	6	5.0	1.00	1	1
Percentage of CIOs in office at least 3 years	15	14	23	25	0	0	19

Source: GAO analysis of agency data.

Note: CIOs who moved from acting to permanent status have been treated as if they were permanent the entire time, and calculations were performed on their aggregated time as one length of service. Also, these acting CIOs who became permanent were not included in the acting calculations above.

# Appendix VI: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE  
6000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

AUG 18 2011

Ms. Cynthia Scott  
Assistant Director  
U.S. Government Accountability Office  
Washington, D.C. 20548

Dear Ms. Scott:

The following are the DoD CIO's comments the GAO draft report GAO-11-634, "FEDERAL CHIEF INFORMATION OFFICERS: Opportunities Exist to Improve Role in Information Technology Management" dated July 19, 2011 (GAO Code 310951).

The Department concurs with the GAO recommendation that the Director OMB issue guidance to agencies, requiring that CIOs' responsibilities and authority, as defined in law, are fully implemented and that appropriate reporting mechanisms are established to validate that this has been accomplished. The Department further notes that Director OMB has taken the first steps in addressing the importance of these issues in his August 8, 2011, memo, "Chief Information Officer Authorities."

Further, while current and former CIOs, as well as the Federal CIO, did not identify legislative changes needed to enhance CIOs' authority and generally felt that existing law provides sufficient authority, the Department (DoD CIO) believes there are legislative opportunities to clarify and strengthen CIO responsibilities and authorities that should be pursued. The most helpful of these would be a deconfliction of potentially overlapping responsibilities between the CIO and various other statutory officials, such as Chief Management Officers, Chief Performance Officers, Chief Acquisition Officers, and Chief Privacy Officers. The Department is currently revising the DoD CIO charter and other policies to address this issue internally, but there would be great value in having a clarified legislative basis for these CIO responsibilities and authorities.

Sincerely,

A handwritten signature in black ink, appearing to read "Teresa M. Takai".

Teresa M. Takai

# Appendix VII: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

August 19, 2011

Valerie C. Melvin  
Director, Information Management and Human Capital Issues  
441 G Street, NW  
U.S. Government Accountability Office  
Washington, DC 20548

Re: Draft Report GAO-11-634, "FEDERAL CHIEF INFORMATION OFFICERS:  
Opportunities Exist to Improve Role in Information Technology Management"

Dear Ms. Melvin:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

Although the report does not contain any recommendations directed at DHS, the Department remains committed to working with the Office of Management and Budget and other relevant stakeholders to address the challenges agency Chief Information Officers face and increase the effectiveness of their efforts.

Again, thank you for the opportunity to review and comment on this draft report. We look forward to working with you on future Homeland Security issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim H. Crumpacker".

Jim H. Crumpacker  
Director  
Departmental GAO/OIG Liaison Office

# Appendix VIII: Comments from the Office of Personnel Management



Chief Information  
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

July 28, 2011

Cynthia Scott, Assistant Director  
Information Management and Human Capital Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20548


OPM appreciates the opportunity to comment on the draft report, Federal Chief Information Officers, Opportunities Exist to Improve Role in Information Technology Management, GAO-11-634 regarding the role of Federal CIOs in meeting agency Information Resource Management (IRM) and Information Technology (IT) responsibilities. As you point out, "IT has the potential to enable federal agencies to accomplish their missions more quickly, effectively and economically...The CIO position was established by Congress to serve as a focal point for IT within an agency." OPM agrees that the CIO plays a critical, strategic role in ensuring every agency serves the American people well.

Under this Administration, OPM has elevated the CIO position and brought it more in line with the original vision of the Clinger-Cohen Act (CCA). Previously, the CIO was buried beneath multiple layers of management, giving the Director little visibility into the health of OPM's many IT investments. Also, several areas of CIO responsibility under CCA - including some IT infrastructure functions - were managed by other parts of the agency. Director Berry consolidated these functions during reorganization early in his tenure and made the CIO a direct report. As a result, IT is better managed, more accountable and the CIO is a strategic player with a seat at the executive table.

Today, all areas of IT and IRM fall within the CIO's purview at OPM. The one exception is that the statistical policy and coordination is primarily handled by OPM's Planning and Policy Analysis organization but with strong links to the CIO's office for technical direction and support. We have seen dramatic improvements in the way IT and IRM are managed and our IT investments are in better shape than ever before.

Because of our own experience, we concur with your recommendation that OMB ensure that all agencies fully implement the organizational changes necessary to make the CIO role function the way it was designed. We also concur that establishing processes for documenting internal lessons learned and best practices regarding the management of IT

and IRM would benefit the federal government as a whole. We look forward to OMB's concurrence on these items.

  
Matthew E. Perry  
Chief Information Officer

---

# Appendix IX: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Valerie C. Melvin (202) 512-6304 or [melvinv@gao.gov](mailto:melvinv@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, key contributions were made to this report by Cynthia J. Scott (Assistant Director); Michael Alexander; Cortland Bradford; Virginia Chanley; James Crimmer, Jr.; Neil Doherty; Ashfaq Huda; Lee McCracken; David Plocher; David A. Powner; Meredith R. Raymond; John M. Resser; Eric Trout; Christy Tyson; Walter Vance; and Merry Woo.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

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

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

