United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Friday,
March 24, 2000

CHIEF INFORMATION OFFICERS

Implementing Effective CIO Organizations

Statement of David L. McClure
Associate Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000327 048

GAO
Accountability * Integrity * Reliability

GAO/T-AIMD-00-128

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the role of chief information officers (CIOs) in the federal government. As you know, Mr. Chairman, the rapid pace of technological change and innovation has offered unprecedented opportunities for the government to use information technology to improve operational performance, reduce costs, and enhance service responsiveness to the public. Yet, at the same time, it has raised a range of thorny issues surrounding managing and integrating complex information management (IM) processes; computer hardware and software; telecommunications networks; and, most important, aligning IT with business needs. Consequently, it is increasingly critical that federal agencies have effective leadership and focused management control over the government's $38 billion in annual spending on information management and technology that goes beyond what would be required solely in a technical support function.

Since the passage of the Clinger-Cohen Act in early 1996, all 24 major cabinet departments and executive agencies have appointed CIOs. Spurred by the Y2K computing problem, many have also begun implementing essential information management processes, such as IT investment management controls, cost estimation processes, and IT architectures. In light of these developments, I would like to briefly touch upon the progress that has been made in establishing federal CIOs and the challenges that remain in achieving the long-term success of these positions. At the same time, I will point out that in order to reap the full benefits of these reforms, more remains to be done to ensure that federal CIOs establish themselves as effective information management leaders, build credible IM organizations, and deliver high-value IT investment results. I also want to introduce an important study we have just completed, entitled *Maximizing the Success of Chief Information Officers – Learning From Leading Organizations*, which can be used to help address the challenges surrounding CIOs. We are publicly releasing this study today; it is based on the best practices of prominent private and state government organizations.[1] The report suggests ways federal agencies can go about ensuring that CIO functions are effectively integrated into overall performance-based and accountability management approaches.

[1]*Executive Guide: Maximizing the Success of Chief Information Officers: Learning From Leading Organizations, Exposure Draft* (GAO/AIMD-00-83, March 2000).

Progress Made In Establishing Federal CIO Positions

To reap the full benefits of new technologies, federal agencies must have effective information management leaders who can transform IT dollars into prudent investments that achieve cost savings, increase productivity, and improve the timeliness and quality of service delivery. This was widely recognized by the Congress in the 1990s as it worked in conjunction with the administration to craft several key information management reform laws, notably the Federal Acquisition Streamlining Act of 1994, the revision of the Paperwork Reduction Act (PRA) in 1995, and the Clinger-Cohen Act of 1996. Other than the Computer Security Act of 1987, these were the first major information management reforms instituted in the federal government since 1980. The Clinger-Cohen Act, for example, required major departments and agencies to appoint CIOs and implement IT management reforms largely grounded in successful commercial IT management practices.[2] In particular, the act established CIO positions that report directly to the agency heads and have IM as a primary function. As noted below, the CIOs are responsible for a wide range of strategic and tactical information management activities outlined in the Clinger-Cohen Act, such as developing architectures, managing and measuring the performance of IT investment portfolios, and assisting in work process improvements. This mirrors the evolution of the CIO position in industry where it has largely moved from solely a technical support focus to a much more executive and strategic level position.

[2]The fiscal year 1997 Omnibus Consolidated Appropriations Act, Public Law 104-208, renamed both Division D (the Federal Acquisition Reform Act) and E (the Information Technology Management Reform Act) of the 1996 DOD Authorization Act, Public Law 104-106, as the "Clinger-Cohen Act of 1996."

Key Clinger-Cohen Requirements for the CIO

- Work with the agency head and senior program managers to implement effective information management to achieve the agency's strategic goals.
- Assist the agency head in establishing a sound investment process to select, control, and evaluate IT spending for costs, risks and benefits.
- Promote improvements to the work processes used by the agency to carry out its programs.
- Increase the value of the agency's information resources by implementing an integrated agencywide technology architecture.
- Strengthen the agency's knowledge, skills, and capabilities to manage information resources effectively.

Effective selection and positioning of CIOs can make a real difference in building the institutional capacity and structure needed to implement the management practices embodied in Clinger-Cohen and PRA.[3] But the position is both relatively new and evolving in the federal government, and agency leaders face many challenges from the growing expectations for dramatic improvements in implementing improved IT management practices and demonstrating cost-effective results. Just finding an effective CIO can be a difficult task, since the individual must combine a number of strengths, including leadership ability, technical skills, an understanding of business operations, and good communications and negotiation skills. Also, the individual selected must match the specific needs of the agency, which must be determined by the agency head based on the agency's mission and strategic plan. The CIO must recognize the need to work as a partner with other business or program executives and to build credibility in order to be accepted as a full participant in the development of new

[3]The PRA of 1980 took the first step toward today's CIO position by designating senior information resources management positions in major departments and agencies. The revision of PRA in 1996, required agencies to indicate in strategic IRM plans how they were applying information resources to improve productivity, efficiency, and effectiveness of government programs, including the delivery of services to the public.

organizational systems and processes and to achieve successful outcomes with IT investments.

Even with the right person in place, the agency head must make a commitment to the success of the CIO by assuring that adequate resources are available and a constructive management framework is in place for implementing agencywide IT initiatives. The resolution of problems founded in unsound investment control processes, poor project management, and weak software development and acquisition capabilities requires executive commitment and active support.

CIOs' progress in working with agency executives to meet these challenges has been mixed. On the positive side, responding to the Year 2000 (Y2K) date conversion challenge helped most agency leaders recognize the importance of consistent and persistent top management attention to information management and technology issues.[4] Progress has been made in strengthening IT management capabilities in order to rectify past failures with costly modernization efforts, e.g., by developing IT architectures, strengthening cost-estimating processes, and improving software acquisition capabilities.[5] In addition, in responding to Y2K, many agencies developed inventories of their information systems, linked those systems to agency core business processes, and jettisoned systems of marginal value.[6] Moreover, more agencies have established much-needed IT policies in areas such as system configuration management, risk management, and software testing.

According to officials at the Office of Management and Budget (OMB), the Y2K problem also gave agency CIOs a "crash course" in how to accomplish projects. Many CIOs were relatively new in their positions and expediting Y2K efforts required many of them to quickly gain an understanding of their agency's systems, work extensively with agency program managers

[4] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999)

[5] *Tax Systems Modernization: Blueprint Is A Good Start But Not Yet Sufficiently Complete to Build or Acquire Systems* (GAO/AIMD/GGD-98-54, February 24, 1998); *Major Management Challenges and Program Risks: A Governmentwide Perspective* (GAO/OGC-99-1, January 1999); *Customs Service Modernization: Actions Initiated to Correct ACE Management and Technical Weaknesses* (GAO/T-AIMD-99-186, May 13, 1999); *Federal Aviation Administration: Challenges in Modernizing the Agency* (GAO/T-RCED/AIMD-00-87, February 3, 2000).

[6] *Year 2000 Computing Challenge: Leadership and Partnerships Result in Limited Rollover Disruptions* (GAO/T-AIMD-00-70, January 27, 2000).

organizational systems and processes and to achieve successful outcomes with IT investments.

Even with the right person in place, the agency head must make a commitment to the success of the CIO by assuring that adequate resources are available and a constructive management framework is in place for implementing agencywide IT initiatives. The resolution of problems founded in unsound investment control processes, poor project management, and weak software development and acquisition capabilities requires executive commitment and active support.

CIOs' progress in working with agency executives to meet these challenges has been mixed. On the positive side, responding to the Year 2000 (Y2K) date conversion challenge helped most agency leaders recognize the importance of consistent and persistent top management attention to information management and technology issues.[4] Progress has been made in strengthening IT management capabilities in order to rectify past failures with costly modernization efforts, e.g., by developing IT architectures, strengthening cost-estimating processes, and improving software acquisition capabilities.[5] In addition, in responding to Y2K, many agencies developed inventories of their information systems, linked those systems to agency core business processes, and jettisoned systems of marginal value.[6] Moreover, more agencies have established much-needed IT policies in areas such as system configuration management, risk management, and software testing.

According to officials at the Office of Management and Budget (OMB), the Y2K problem also gave agency CIOs a "crash course" in how to accomplish projects. Many CIOs were relatively new in their positions and expediting Y2K efforts required many of them to quickly gain an understanding of their agency's systems, work extensively with agency program managers

[4] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999)

[5] *Tax Systems Modernization: Blueprint Is A Good Start But Not Yet Sufficiently Complete to Build or Acquire Systems* (GAO/AIMD/GGD-98-54, February 24, 1998); *Major Management Challenges and Program Risks: A Governmentwide Perspective* (GAO/OGC-99-1, January 1999); *Customs Service Modernization: Actions Initiated to Correct ACE Management and Technical Weaknesses* (GAO/T-AIMD-99-186, May 13, 1999); *Federal Aviation Administration: Challenges in Modernizing the Agency* (GAO/T-RCED/AIMD-00-87, February 3, 2000).

[6] *Year 2000 Computing Challenge: Leadership and Partnerships Result in Limited Rollover Disruptions* (GAO/T-AIMD-00-70, January 27, 2000).

and chief financial officers (CFOs), and become familiar with budgeting and financial management practices.[7]

The Federal CIO Council has also facilitated positive developments.[8] For example, the Council has been working actively with the Office of Personnel Management to develop special pay rates for hard-to-hire IT professionals. It has facilitated the development of a web-based information consolidation tool, which provides a standard IT budget reporting format and should assist agencies in linking their internal planning, budgeting, and management of IT resources. The Council also assisted administration officials in tracking the progress of Presidential Decision Directive 63, which tasked federal agencies with developing critical infrastructure protection plans, identification and evaluation of information security standards, and best practices and efforts to build communication links with the private sector. Further, in addressing the Y2K challenge, the Council participated in governmentwide efforts to develop best practices for Y2K conversion and to address important issues such as acquisition and Y2K product standards, data exchange issues, telecommunications, buildings, biomedical and laboratory equipment, and international issues.

Still, agencies face incredible challenges in effectively managing their IT investments and in assuring that these investments make the maximum contribution to mission performance that is possible. Some of our recent reviews have found that fundamental IT investment processes are incomplete and not working consistently to help achieve better project outcomes. For example, IT portfolio selection, control, and evaluation processes and performance metrics have not been developed to gauge the progress of investments or their contribution to program outcomes.[9]

---

[7] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

[8] The Council was created by Executive Order 13011, July 16, 1996, *Federal Information Technology*. The Council is to be the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council is to make recommendations and provide advice to agencies and organizations but does not have policy authority. The order also created the Information Technology Services Board to identify and promote the development of innovative technologies, standards, and practices among agencies, state and local governments, and the private sector.

[9] *Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk* (GAO/AIMD-98-5, October 20, 1997); *Indian Trust Funds: Interior Lacks Assurance That Trust Improvement Plan Will Be Effective* (GAO/AIMD-99-53, April 28, 1999); and *Air Traffic Control: FAA's Modernization Investment Management Approach Could Be Strengthened* (GAO/RCED/AIMD-99-88, April 30, 1999).

Acquisitions may be executed faster, but in many cases the link to program performance is lost so the real value of the investment cannot be determined. In short, more clarity could be given to how IT investments are being or will be used to improve performance or help achieve specific agency goals and ensuring that better data exists to guide informed decisions. Other common problem areas include inadequate progress in designing and implementing IT architectures before proceeding with massive modernization efforts and immature software development, cost estimation, and acquisition practices.[10] These are areas where the agency heads were assigned specific responsibility in the PRA and in the Clinger-Cohen Act, and for which CIOs were appointed to help rectify poor agency track records.

Information security is another widespread and growing problem confronting federal CIOs. A rash of break-ins at federal websites and disruptions caused by the Melissa computer virus and other malicious viruses sent via the Internet recently highlighted this concern. However, our reviews show that this problem runs much deeper. In particular, our October 1999 analysis of our own and inspector general audits found that 22 of the largest federal agencies were not adequately protecting critical federal operations and assets from computer-based attacks.[11] Among other things, we found that agencies are lacking the strong, centralized leadership needed to protect critical information and assets as well as sound security planning, effective control mechanisms, and speedy response to security breakdowns.[12] These weaknesses pose enormous risks to our computer systems and, more important to the critical operations and infrastructure they support, such as telecommunications; power distribution, national defense, and law enforcement; government services; and emergency services. In the case of computer security, too,

[10] *Major Management Challenges and Program Risks: A Governmentwide Perspective* (GAO/OGC-99-1, January 1999).

[11] *Information Security: Weaknesses at 22 Agencies* (GAO/AIMD-00-32R, November 10, 1999) and *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations* (GAO/T-AIMD-00-7, October 6, 1999).

[12] *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999); *Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999); *Audit of the Department of State's 1997 and 1998 Principal Financial Statements*, Leonard G. Birnbaum and Company, LLP, August 9, 1999; *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4, 1999); *IRS Systems Security: Although Serious Improvements Made, Tax Processing Operations and Data Still at Serious Risk* (GAO/AIMD-99-38, December 14, 1998); and *Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-4, October 4, 1999).

the responsibility has been given to the agency heads by the PRA and Clinger-Cohen Act with CIOs to provide support.

Clearly, more remains to be done to realize the full potential of CIOs as information management leaders, to build CIO organizations that have the credibility needed to be successful; to define the measures necessary to gauge this success and demonstrate results, and to put in place the structure for organizing information management to meet pressing business needs. The CIO executive guide that we are releasing today is designed to help resolve these challenges. Through our research and interviews with CIOs and other executives in case study organizations, we have developed a framework of critical success factors and leading principles. Federal agencies can turn to this guide for pragmatic assistance in leveraging the CIO position.

Learning to Maximize the Success of CIO Organizations

Mr. Chairman, our research has demonstrated that CIOs of leading organizations use a consistent set of IM principles to execute their responsibilities successfully. These principles, listed below, span a broad range of management imperatives, from executive leadership and change management through organizational design and workforce development.

Some principles need to be addressed by top executives across the organization, rather than by the CIO. For example, along with other top executives, the chief executive officer (CEO) must recognize the role of IM in creating value to the business before appointing a CIO. In addition, the CEO must also undertake responsibility for defining and instituting the CIO position. The other principles are squarely within the domain of the CIO. For example, the CIO must take full responsibility for ensuring the credibility of the IM organization. While other leaders can contribute to this principle, the CIO must be seen as the leader of the unit and must consistently raise the visibility and demonstrate the value of the IM organization across the enterprise. Overall, the principles are strikingly simple and strongly supported by a wide range of other CIO-based research. Nevertheless, consistent attention and commitment often remains elusive and pinpoints the notable difference between leading organizations and others.

Six Principles of CIO Management

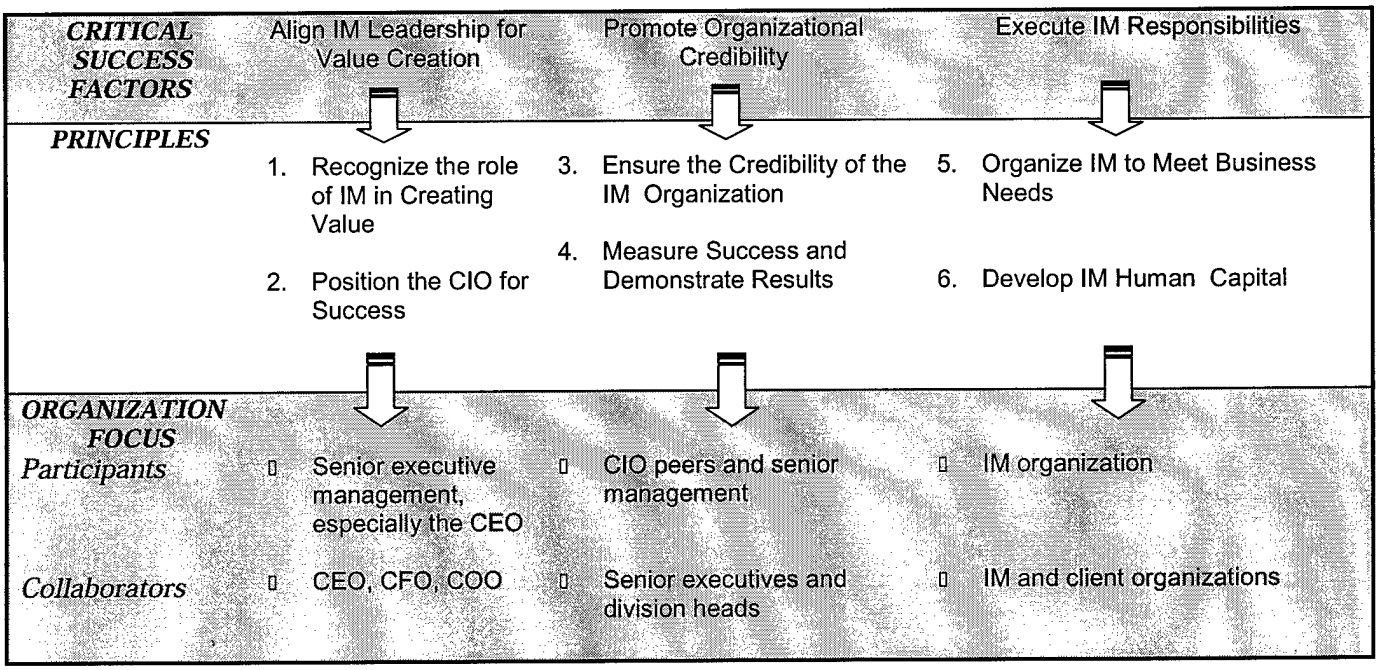
- Recognize the role of IM in creating value
- Position the CIO for success
- Ensure the credibility of the IM organization
- Measure success and demonstrate results
- Organize IM to meet business needs
- Develop IM human capital

Let me also underscore, Mr. Chairman, that the principles are most effective when implemented together in a mutually reinforcing manner. As ad hoc efforts, each principle addresses a single aspect that while necessary, is not sufficient for success by itself. And the failure to execute a single principle may render others less effective. Nevertheless, organizations may find it more feasible to address one principle before another.

The Foundations for Achieving CIO Success: Consistent Critical Success Factors and Key Characteristics

The six principles we identified naturally fell into three critical success factors that are useful for understanding issues of implementation and impact. These critical success factors are (1) align IM leadership for value creation, (2) promote organizational credibility, and (3) execute IM responsibilities. These success factors provide focus for the CIO when planning how to address the six principles. As the CIO develops strategies for approaching each of the six principles, he or she must consider who else in the organization must be involved in the leadership and what parts of the organization must be involved in the implementation. Within each critical success factor, a specific level of the organization contributes to the leadership, along with the CIO, and a specific part of the organization is involved in carrying out the activities that lead to the successful execution of the factor. For example, to align IM leadership for value creation, the CEO and most other senior executives must actively endorse the CIO and demonstrate the CIO's role in the strategic management of the organization. The second success factor requires the collaboration of the next lower layer of management where IM successes will be observed. Finally, the third factor is where the rubber hits the road, and the IM organization itself must demonstrate its effectiveness.

Figure 1: Critical Success Factors for CIOs



Each principle identified in our guide is also defined by key characteristics. These key characteristics represent the specific approaches we observed that contribute to the success of the CIO. For example, to ensure the credibility of the IM organization, successful organizations ensure that (1) the CIO model complements organizational and business needs, (2) the CIO's roles, responsibilities, and accountabilities are clearly defined, and (3) the CIO has the right technical and management skills to do the job. To define performance measures, IM managers generally engage both their internal and external partners and customers and continually work at establishing feedback between performance measurement and business processes.

As CIOs or senior agency executives use our guide, they may want to compare their organization to these key characteristics to assess the extent to which their organization resembles those we visited in the development of our guide. They may also gain insight into what aspects of their organization they should address as they work to enhance the effectiveness of their CIO position. Our guide also presents case studies illustrating how these key practices are employed within specific

organizations. And it suggests specific strategies for implementing both principles and characteristics.

Table 1: Key Characteristics of CIO Principles

	Principles	*Key Characteristics*
Recognize the role of IM in creating value	Instituting an effective CIO organization does not start with the selection or placement of an IM leader, or setting up a structure for managing information resources and activities. Rather, it begins with consideration of the role of IM and how vital it is to accomplishing mission objectives.	• IM organization functions and processes are incorporated into the overall business process. • Mechanisms and structures are adopted that facilitate an understanding of IM and its impact on the organization's overall strategic direction.
Position the CIO for success	There is no one way to establish a CIO position, but there are a number of practices and strategies that senior managers in leading organizations use to help define and institute their CIO positions to effectively meet business needs.	• The CIO model is consistent with organizational and business needs. • The roles, responsibilities, and accountabilities of the CIO are clearly defined. • The CIO has the right technical and management skills to meet business needs. • The CIO is a full member of the senior management team.
Ensure the credibility of the IM organization	Instituting a CIO position consistent with organization needs and finding a credible leader to fill the job are no guarantee of CIO success. CIOs themselves must employ strategies to legitimize their roles and successfully collaborate with their business counterparts to guide IM solutions and meet mission needs.	• The CIO has a legitimate and influential role in leading top managers to apply IM to meet business objectives. • The CIO has the commitment and trust of line management. • The CIO accomplishes quick, high-impact, and visible IM successes in balance with long-term strategies. • The CIO learns from and partners with successful leaders in the organization.

	Principles	Key Characteristics
Measure success and demonstrate results	In many organizations, the value of IM is considered difficult to measure. However, it has become increasingly evident that without a measurement process where results can be demonstrated, not only is IM at a disadvantage when competing for scarce resources, but also when making its case in support of IM initiatives.	• IM managers engage both their internal and external partners and customers when defining measures. • Managers at all levels ensure that technical measures are balanced with business measures. • Managers continually work at establishing active feedback between performance measurement and business processes.
Organize IM to meet business needs	The IM organization must provide effective, responsive support to the business through efficient allocation of resources and the day-to-day execution of responsibilities.	• The IM organization has a clear understanding of its responsibilities. • The extent of decentralization of IM resources and decision-making is driven by business needs. • The structure of the IM organization is flexible enough to adapt to changing business needs. • The IM organization executes its responsibilities reliably and efficiently.
Develop IM human capital	Given prevailing market forces and internal legacies, the IM organization must provide an effective, responsive IM workforce to help accomplish mission and goals.	• The IM organization identifies necessary skills. • The IM organization develops innovative ways to attract and retain talent. • The IM organization provides needed training, tools, and methods.

How Leading Organizations Compare With Federal CIO Management Practices

In our discussions with half of the Federal CIO Council members, they agreed that the six primary principles emerging from our study were relevant to the issues and challenges confronting them. However, the specific approaches to executing those principles differed, and for a number of principles, the federal sector seemed to not provide much focus at all. For example, while leading organizations generally define the role and authority of their CIO position carefully given the needs of the enterprise, and then select a CIO with the skills to meet the challenge,

senior executives in the federal sector do not seem to go through the same process of linking CIO type and skills to agency needs. In addition, leading organizations work hard to forge partnerships at the top levels of the organization, something seen less frequently in the federal sector.

This lack of attention to the CIO as the focal point of IM practice in the agency extends to the failure of agency heads to include their CIOs in executive business decision-making. In the federal government setting, IM is still too often treated as purely a technical support function rather than a strategic asset critical to improving mission performance and achieving more cost-effective results. As a result, the CIO's role is often further from the strategic planning of the organization than in the organizations we contacted for our guide. Moreover, federal organizations are often less flexible in reassigning IM staff and structuring capabilities across business and technology lines due to the highly decentralized IM responsibilities found in many large agencies.

Also, the relative inflexibility of federal pay scales makes it difficult to attract and retain the highly skilled IT professionals required to develop and support the systems being proposed. I will be discussing these and other constraints further momentarily, but I would like to point out that such challenges tend to slow the progress of implementing other principles.

Interestingly, the practices of federal CIOs tended to be most similar to those CIOs in our study in those principles in which CIOs could exert the most personal control. That is, federal CIOs tend to use the same approach to building credibility within the enterprise as our case study CIOs did. In addition, both groups of CIOs tend to have similar problems with performance measures and demonstrating results. Our case study CIOs had made more advances in building links between IM and business objectives, but the measures themselves are still evolving. On the federal side, the ties to mission performance are not as strong, perhaps because of a lack of collaboration between the program areas and the IM organization in the development of mission requirements, though provisions of the Clinger-Cohen Act are providing the motivation to improve this process.

Table 2: How Leading Organizations Compare With Federal Practices

Critical Success Factors	Principle	What a Leading Organization Does	What the Federal Government Does
Align IM Leadership for Value Creation	*Recognize the Role of IM in Creating Value*	• CEOs and governors ensure that the IM organization is a key business player • CIO is part of the executive decision-making process	• IM generally still viewed as a support function instead of as a strategic activity • CIO is not always involved in strategic and policy-making decisions
	Position the CIO for Success	• Defines clear CIO role and authorities • Matches CIO type and skills set with business needs • Forges CIO partnership with CEO and other senior executives	• Does not always clearly define CIO role or authority • Does not always match CIO selection with agency needs • Does not always provide executive support for the CIO position
Promote Organizational Credibility	*Ensure the Credibility of the IM Organization*	• CIO builds credibility through effective IM leadership, good working relationships, track records, and partnering with customers and peers	• Uses practices similar to leading organizations
	Measure Success and Demonstrate Results	• Strong links exist between business objectives and performance measures • Performance management structure still evolving	• Weak links between agency goals and IM/IT performance measures • Required annual performance plans still in preliminary stages
Execute IM Responsibilities	*Organize IM to Meet Business Needs*	• Reassigns IT staff as needed to best serve interests of customers • Structures the organization along business lines as well as IM functional areas	• Tries to meet needs of customers with a fixed organizational structure • Structures the organization primarily along IM functional areas
	Develop IM Human Capital	• Maintains up-to-date professional skills in technology management • Outsources entry-level positions but largely hires at all levels of experience	• Provides limited amount of training in technology management • Assumes entry-level IM staff will remain in federal service as a career

Additional Constraints on Federal CIOs Warrant Further Attention

Our interviews with federal CIOs and agency executives helped to highlight several aspects of the environment in which federal CIOs operate that are, in some respects, not common in private industry. In some cases, analogies do exist outside the federal sector, but it is important to understand these differences as contextual factors affecting the speed, pace, and direction of CIO integration in the federal government. As such, these factors may warrant further dialogue and empirical study. The outcomes of these discussions and reviews can form the basis for a

constructive dialogue between the Congress and the executive branch on future revisions to IT management statutes and executive branch policies.

- First, senior executive management in the federal sector can differ significantly from the private sector. The agency head and other top executives are political appointees who are often more focused on national policy issues than building capabilities essential for achieving the desired strategic and program outcomes. This can deny the CIO the CEO-level support that is so critical for the successful integration of IM into the core business or mission functions. The Clinger-Cohen Act addresses this situation by holding the agency heads accountable for IT and requiring the CIOs to work with other executives in the management of their agencies' information resources.

- Second, the federal budget process can create funding challenges for the federal CIO that are not found in the private sector. For example, certain information projects may be mandated or legislated, so the CIO does not have the flexibility to decide whether to pursue them. This ties up IT investment funds that might otherwise have been spent on other priorities. Additionally, the annual budget cycle of the federal government creates a great deal of uncertainty in funding levels available year-to-year, particularly when IT dollars are part of overall agency discretionary spending. The multitude of players in the budget process can also lead to unexpected changes in funding and the loss of the connection between budget and achievement of agency mission. This can create dynamic decision-making challenges for long-term investment strategies. Further, IT funds are often contained within the appropriations for a specific program, making them less visible. As a result, the CIO may not have control or direct oversight of key parts of the IT funding within the agency. The Clinger-Cohen Act addresses this by requiring fact-based decision-making for project initiation and control. OMB is charged with reviewing the decision support and inspecting the link between budget proposal and expected performance outcomes.

- Third, human capital decisions in the federal sector are often constrained relative to the flexibility found elsewhere. Current federal IM job descriptions do not match the occupations recognized in the IM industry today. Funds for skill refreshment are often among the first to be scaled back in across-the-board budget cuts. The Office of Personnel Management has also found IM salaries in the federal government to be lower than in the private sector and incentives available in the private sector do not exist in the federal government.

- Fourth, the federal CIO may direct an organization without the full range of functional responsibilities that would typically be a CIO's responsibility in the private sector. For example, some federal CIOs are in charge of larger policy and oversight functions with little operational responsibility. While this may be an appropriate model for some agencies, it is critical that any model be matched with the overall needs of the agency and legislative responsibilities in mind.

- Fifth, the range of responsibilities, as defined by legislation, that accrue to the CIO are very broad in the federal sector, including areas like records management, paperwork burden reduction and clearance, and Freedom of Information Act requirements, for which there is little parallel in the private sector. While federal CIOs often may not have the operational responsibility for the full range of activities covered in legislation, they are charged with ensuring that these functions are effectively performed.

Leadership turnover; shifts in business direction, priorities, and emphasis; changing funding levels; and human capital issues are real issues in all organizations—public and private. As such, these constraints should not be viewed as reasons for why the federal CIO cannot be successful. Instead, these constraints should be recognized and anticipated so that effective management approaches can be put in place to mitigate risks and address accountability.

Concluding Remarks

Mr. Chairman, as the federal government moves to fully embrace the digital age and focuses on electronic government initiatives, leadership in the management of the government's information resources is of paramount importance. Yet, as our study shows, as a single individual, a CIO cannot ensure the successful implementation of information management reforms. Rather, the CIO must be buttressed by the full support of agency heads, the commitment of line managers, clearly defined roles and responsibilities, effective measures of performance, highly skilled and motivated IT professionals, and a range of other factors.

The practices and key characteristics defined in our CIO guide can put agencies on the right path toward incorporating these ingredients. Moreover, they can help agencies and their CIOs to identify and correct underlying IM weaknesses that have undermined their modernization initiatives. They can even help ensure that agencies will be well positioned to take advantage of cutting-edge technologies in order to transform service delivery and performance. However, implementing the practices alone is not enough. To achieve real success, agency executives as well as the Congress must provide sustained support and attention to facilitating

CIO effectiveness and addressing any structural challenges facing CIOs. Using this support, CIOs themselves must be now focused on results—making sure that IT investments make their agencies more innovative, efficient, and responsive.

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

Contact and Acknowledgments

For future contacts regarding this testimony, please contact David L. McClure at (202) 512-6257. Individuals making key contributions to this testimony included Cristina Chaplain, Lester Diamond, Tamra Goldstein, Sondra McCauley, Tom Noone, and Tomas Ramirez.

(511704)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)