United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10 a.m.
Monday,
October 27, 1997

CHIEF INFORMATION OFFICERS

Ensuring Strong Leadership and an Effective Council

Statement of Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the importance of having strong Chief Information Officers (CIOs) at major federal agencies[1] and ensuring an effective CIO Council to help bring about much-needed reforms in the government's management of information technology (IT). During the last decade, much attention has been focused on serious problems with federal information technology projects. The picture that unfolded year after year was bleak: multimillion dollar and, in some cases, billion dollar system development efforts routinely came in over cost, behind schedule, and lacking in promised capabilities. In addition to wasting resources, these disappointing efforts seriously weakened agencies' abilities to meet mission goals and improve operational efficiency.[2]

To help reverse this trend, GAO embarked on a concerted effort to learn how leading private and public sector organizations controlled system development projects and successfully applied technology to improve their performance. Our resulting study identified a specific set of strategic practices that these organizations use to improve performance through information management.[3] Based upon our work and that of others, the Congress, in conjunction with the Administration, crafted two recent landmark reforms in federal information management: the Paperwork Reduction Act (PRA) of 1995 and the Clinger-Cohen Act of 1996. These reforms encompass many important elements identified in our best practices work, such as establishing more disciplined information technology investment control processes, developing an overall information architecture, and defining measures to show how information technology is contributing to improved program performance.

Central to implementing these reforms is the need to establish effective leadership at each agency. Under the law, agency heads are directly responsible for effective information management, but CIOs play a critical leadership role in driving reforms to help control system development risks, better manage technology spending, and succeed in achieving real,

[1]In this testimony, we use the term "agencies" to refer to both cabinet-level departments and major agencies.

[2]For background on these problems see 1995 High-Risk Series: An Overview (GAO/HR-95-1, February 1995); 1997 High-Risk Series: An Overview (GAO/HR-97-1, February 1997); Paperwork Reduction Act: Opportunity to Strengthen Government's Management of Information and Technology (GAO/T-AIMD/GGD-94-126, May 19, 1994); and Government Reform: Legislation Would Strengthen Federal Management of Information and Technology (GAO/T-AIMD-95-205, July 25, 1995).

[3]Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994).

measurable improvements in agency performance. Furthermore, the agency CIOs, working collectively as a Council, have a critical leadership role to play in addressing governmentwide technology issues and advising the Office of Management and Budget (OMB) on policies and standards needed to successfully implement legislative reforms.

The challenge facing the federal government today is to provide the type of leadership needed to implement information technology reforms as rapidly as possible. Although we are beginning to see some progress, agencies still have a long way to go to translate legislative mandates into day-to-day management reality. The following sections offer our observations on the status of efforts to promote effective CIO leadership and the challenges and opportunities faced by the CIO Council. Our views are based not only on our work in the technology area, but also on our experiences in evaluating the implementation of other major management reforms, such as the Chief Financial Officers (CFO) Act of 1990 and the Government Performance and Results Act (Results Act) of 1993.

Ensuring That CIOs Fulfill a Critical Leadership Role

Senior executives in the successful organizations we studied were personally committed to improving the management of technology. The PRA and the Clinger-Cohen Act make federal agency heads directly responsible for establishing goals and measuring progress in improving the use of information technology to enhance the productivity and efficiency of their agency's operations. To help them with their major information management responsibilities, the reform legislation directs the heads of the major agencies to appoint CIOs.[4] The legislation assigns a wide range of duties and responsibilities to CIOs, foremost of which are

- working with the agency head and senior program managers to implement effective information management to achieve the agency's strategic goals;
- helping to establish a sound investment review process to select, control, and evaluate spending for information technology;
- promoting improvements to the work processes used by the agency to carry out its programs;

[4]Under the Clinger-Cohen Act, CIO positions were designated at the same 24 agencies where the CFO Act (as amended) established chief financial officer positions. In addition, CIOs were created at the Army, Navy, and Air Force. Together, these 27 agencies account for nearly all fiscal year 1997 executive branch outlays of about $1.6 trillion.

- increasing the value of the agency's information resources by implementing an integrated agencywide technology architecture;[5] and
- strengthening the agency's knowledge, skills, and capabilities to effectively manage information resources, deal with emerging technology issues, and develop needed systems.

While there are various approaches on how best to use the CIO position to accomplish these duties, the legislative requirements, OMB guidance,[6] and our best practices experience with leading organizations define common tenets for the CIO position. An agency should place its CIO at a senior management level, working as a partner with other senior officials in decision-making on information management issues. Specifically, agencies should

- appoint a CIO with expertise and practical experience in technology management;
- position the CIO as a senior partner reporting directly to the agency head;
- ensure that the CIO's primary responsibilities are for information management;
- have the CIO serve as a bridge between top management, line management, and information management support professionals, working with them to ensure the effective acquisition and management of the information resources needed to support agency programs and missions;
- task the CIO with developing strategies and specific plans for the hiring, training, and professional development of staff in order to build the agency's capability to develop and manage its information resources; and
- support the CIO position with an effective CIO organization and management framework for implementing agencywide information technology initiatives.

Having effective CIOs will make a real difference in building the institutional capacity and structure needed to implement the management practices embodied in the broad set of reforms set out in the PRA and the Clinger-Cohen Act. The CIO must combine a number of strengths, including

[5]A systems architecture is a blueprint, having both a technical and a logical component, to guide and constrain the development and evolution of a collection of related systems. At the logical level, the architecture provides a high-level description of the organizational mission being accomplished, the business functions being performed and the relationships among the functions, the information needed to perform the functions, and the flow of information among functions. At the technical level, the architecture provides the rules and standards needed to ensure that the interrelated systems are built to be interoperable, portable, and maintainable. These include specifications of critical aspects of component systems' hardware, software, communication, data, security, and performance characteristics.

[6]Memorandum for the President's Management Council, "What Makes a Good CIO?" June 28, 1996.

leadership ability, technical skills, an understanding of business operations, and good communications and negotiation skills. For this reason, finding an effective CIO can be a difficult task. Agencies faced a similar difficulty in trying to find qualified chief financial officers to implement the CFO Act's financial management reforms. It took time and concerted effort by the Administration, the CFO Council, and the Congress to get strong, capable leaders into the CFO positions.

Shortly after the Clinger-Cohen Act went into effect, OMB evaluated the status of CIO appointments at the 27 agencies. OMB noted that at several agencies, the CIO's duties, qualifications, and 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. These CIOs also had exposure to a broad range of technologies, as well as knowledge of government budgeting and procurement processes and information management laws, regulations, and policies.

However, OMB had concerns about a number of other agencies that had acting CIOs, CIOs whose qualifications did not appear to meet the requirements of the Clinger-Cohen Act, and/or CIOs who did not report directly to the head of the agency. OMB also raised concerns about agencies where the CIOs had other major management responsibilities or where it was unclear whether the CIOs' primary duty was the information resource management function. OMB stated that it would reevaluate the situations at these agencies at a later date, after agencies had time to put permanent CIOs in place or take corrective actions to have their CIO appointment and organizational alignment meet the necessary requirements.

OMB called for updated information on the status of governmentwide CIO appointments in its April 1997 data request on individual agency efforts to implement provisions of the Clinger-Cohen Act.[7] OMB has not yet issued a status report based on this information and subsequent follow-up. In a recent discussion, OMB officials stated that they will provide feedback on individual CIO appointments as part of the fiscal year 1999 budget review process. On the basis of preliminary observations, however, OMB officials stated that they still have some of the same concerns that they had a year ago about CIO positions that have not been filled, have not been properly positioned, or have multiple responsibilities.

[7]OMB Memorandum M-97-12, "Evaluation of Agency Implementation of Capital Planning and Investment Control Processes," April 25, 1997.

It is very important for OMB to follow through on its efforts to assess CIO appointments and resolve outstanding issues. Information technology reforms simply will not work without effective CIO leadership in place. We will continue to monitor this situation to provide our suggestions on actions that need to be taken.

One area that we will focus on during the coming year is CIOs who have major responsibilities in addition to information management. The Clinger-Cohen Act clearly calls for CIOs to have information resources management as their primary duty. We have stressed the importance of this principle in testimonies and, most recently, in our February 1997 high-risk report, in which we emphasized that the CIO's duties should focus sharply on strategic information management issues and not include other major responsibilities.[8] In addition to the escalating demands of rapidly evolving technologies, CIOs are faced with many serious information management issues, any one of which would be a formidable task to address. Taken together, these issues create a daunting body of work for any full-time CIO, much less for one whose time and attention is divided by other responsibilities. As you know, Mr. Chairman, we have reported extensively on a number of these compelling challenges. The following are just a few of these challenges.

- Ensuring that federal operations will not be disrupted by the Year 2000 problem is one of the foremost and most pressing issues facing agencies—one that we have designated as a governmentwide high-risk area. Efforts by this Subcommittee have underscored repeatedly that many agencies are seriously behind schedule in resolving this problem during the next 2 years.[9]
- Poor security management is putting billions of dollars worth of assets at risk of loss and vast amounts of sensitive data at risk of unauthorized disclosure, making it another of our governmentwide high-risk areas. Agencies need to make much better progress in designing and implementing security programs and getting skilled staff in place to

[8]Government Reform: Legislation Would Strengthen Federal Management of Information and Technology (GAO/T-AIMD-95-205, July 25, 1995); Managing Technology: Best Practices Can Improve Performance and Produce Results (GAO/T-AIMD-97-38, January 31, 1997); and High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[9]Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach (GAO/T-AIMD-97-173, September 25, 1997). Among other Year 2000 reports are: Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997); Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997); and Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997).

manage them.[10] This extreme vulnerability has been given added emphasis by the recent Presidential commission report on the growing exposure of U.S. computer networks to exploitation and terrorism.[11]

- Agencies need to develop, maintain, and facilitate integrated systems architectures to guide their system development efforts. We have seen major modernization efforts handicapped by incomplete architectures, such as at the Federal Aviation Administration (FAA) and the Internal Revenue Service (IRS), as well as the departments of Veterans Affairs and Education.[12]
- Agencies need to establish sound information management investment review processes that provide top executives with a systematic, data-driven means to select and control how technology funds are spent. Our reviews of system development and modernization projects, such as the Medicare Transaction System and the four high-risk efforts included in our 1997 High-Risk Series, continue to show the crucial importance of structured investment oversight.[13]
- In our 1997 High-Risk Series we identified 25 high-risk areas covering a wide array of key federal activities, ranging from Medicare fraud to financial management at the Department of Defense. Resolving the problems in these areas depends heavily on improved information management.
- Agencies need to integrate strategic information planning with the overall strategic plan that they must prepare under the Results Act. Our review of recent attempts by agencies to develop sound strategic plans showed very weak linkages between the strategic goals and the information technology needed to support those goals.[14]

[10]Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

[11]The President's Commission on Critical Infrastructure Protection issued its final report to the President on October 20, 1997. The report has not yet been released to the public.

[12]See Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997); Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996); Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997); and Student Financial Aid Information: Systems Architecture Needed to Improve Programs' Efficiency (GAO/AIMD-97-122, July 29, 1997).

[13]Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997). High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997). The four modernization projects on GAO's high-risk list are FAA's air traffic control modernization, the Department of Defense's Corporate Information Management initiative, the National Weather Service modernization, and IRS' Tax Systems Modernization.

[14]Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans (GAO/GGD-97-180, September 16, 1997).

- Agencies must build their staffs' skills and capabilities to react to the rapid developments in information technology, develop needed systems, and oversee the work of systems contractors. Weaknesses in agencies' technology skills bases, especially in the area of software acquisition and development, have been a recurring theme in our reviews of federal information technology projects.[15]

Despite the urgent need to deal with these major challenges, we still see many instances of CIOs who have responsibilities beyond information management. At present, only 12 agencies have CIOs whose responsibilities are focused solely on information management. The other 15 agencies have CIOs with multiple responsibilities. Together, these 15 agencies account for about $19 billion of the nearly $27 billion dollars in annual federal planned obligations for information technology. While some of these CIO's additional responsibilities are minor, in many cases they include major duties, such as financial operations, human resources, procurement, and grants management. At the Department of Defense, for example, the CIO is also the Assistant Secretary for Command, Control, Communications and Intelligence. By asking the CIO to also shoulder a heavy load of programmatic responsibility, it is extremely difficult, if not impossible, for the CIO to devote full attention to information resource management issues. Recognizing this problem, the Department's Task Force on Defense Reform is examining the current structure of the CIO position to ensure that the person can devote full attention to reforming information management within the Department.[16]

We are particularly troubled by agencies that have vested CIO and Chief Financial Officer responsibilities in one person.[17] The challenges facing agencies in both financial and information management are monumental. Each requires full-time leadership by separate individuals with appropriate talent, skills, and experience in these two areas. In financial management, for example, most agencies are still years away from their goal of having

[15]Weather Forecasting: Recommendations to Address New Weather Processing System Development Risks (GAO/AIMD-96-74, May 13, 1996); Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996); Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997); Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997); and Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997).

[16]Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, October 20, 1997).

[17]Commerce, Education, Health and Human Services, Justice, and the Veterans Administration have combined CIOs/CFOs.

reliable, useful, relevant, and timely financial information—an urgently needed step in making our government fiscally responsible.

Because it may be difficult for the CIO of a large department to adequately oversee and manage the specific information needs of the department's major subcomponents, we have also supported the establishment of a CIO structure at the subcomponent and bureau levels.[18] Such a management structure is particularly important in situations where the departmental subcomponents have large information technology budgets or are engaged in major modernization efforts that require the substantial attention and oversight of a CIO. In the Conference Report on the Clinger-Cohen Act, the conferees recognized that agencies may wish to establish CIOs for major subcomponents and bureaus.[19] These subcomponent level CIOs should have responsibilities, authority, and management structures that mirror those of the departmental CIO.

We have reported on instances where the subcomponent CIOs were not organizationally positioned and empowered to discharge key CIO functions. For example, in our reviews of FAA's air traffic control (ATC) modernization, which is expected to cost $34 billion through the year 2003, we found that FAA's CIO was not responsible for developing and enforcing an ATC systems architecture. Instead, FAA had diffused architectural responsibility across a number of organizations. As a result, FAA did not have a complete ATC architecture, which in turn has led to incompatible and unnecessarily expensive and complex ATC systems. Additionally, we found that while FAA's CIO was responsible for ATC software acquisition process maturity and improvement, the CIO lacked the authority to implement and enforce process change. Consequently, we reported that (1) FAA's processes were *ad hoc,* and sometimes chaotic, and not repeatable across ATC projects and (2) its improvement efforts have not produced more disciplined processes. Among other actions, we recommended that FAA establish an effective management structure for developing, maintaining, and enforcing a complete systems architecture and improving software acquisition process improvement and that this

[18]Government Reform: Legislation Would Strengthen Federal Management of Information and Technology (GAO/T-AIMD-95-205, July 25, 1995).

[19]H. R. Conf. Rep. No. 104-450 at 977 (1996).

management structure be similar to the department-level CIO structure prescribed by the Clinger-Cohen Act.[20]

Similarly, in the last few years, we have reported and testified on management and technical weaknesses associated with IRS' Tax Systems Modernization.[21] Among other things, we have noted how important it is for IRS to have a single IRS entity with responsibility for and control over all information systems efforts. Since we first reported on these problems, IRS has taken a number of positive steps to address its problems and consolidate its management control over systems development. However, as we noted in recent briefings to the acting IRS Commissioner and congressional committee staffs, neither the CIO nor any other organizational entity has sufficient authority needed to implement IRS' Systems Life Cycle—its processes and products for managing information technology investments—or enforce architectural compliance agencywide. We will soon be making formal recommendations to IRS to address this issue.

Finally, as we reported to you earlier this year,[22] the problems encountered by the Health Care Financing Administration (HCFA) in its development of the Medicare Transaction System provide another example of the need for strong management over the development and implementation of information systems. In recent testimony on Medicare automated systems,[23] we reemphasized the importance of establishing CIOs and involving them and other senior executives in information management decisions. While HCFA has recently established a CIO and an Information Technology Investment Review Board, the agency has not yet implemented an investment process—including senior management roles

[20]Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997); Air Traffic Control: Improved Cost Information Needed to Make Billion Dollar Modernization Investment Decisions (GAO/AIMD-97-20, January 22, 1997); and Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997).

[21]Tax Administration: IRS' Fiscal Year 1997 Spending, 1997 Filing Season, and Fiscal Year 1998 Budget Request (GAO/T-GGD/AIMD-97-66, March 18, 1997); Internal Revenue Service: Business Operations Need Continued Improvement (GAO/AIMD/GGD-96-152, September 9, 1996); Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996); and Tax Systems Modernization: Management and Technical Weaknesses Must Be Corrected If Modernization Is To Succeed (GAO/AIMD-95-156, July 26, 1995).

[22]Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997) and Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997).

[23]Medicare Automated Systems: Weaknesses in Managing Information Technology Hinder Fight Against Fraud and Abuse (GAO/T-AIMD-97-176, September 29, 1997).

and responsibilities—that governs the selection, control, and evaluation of IT investments. Consequently, we have recommended that HCFA establish an investment management approach that explicitly links the roles and responsibilities of the CIO and Investment Review Board to relevant legislative mandates and requirements. Such actions are essential to ensure that HCFA's—or any agency's—information technology initiatives are cost-effective and serve its mission.

Establishing a Strategic Direction for the CIO Council

Although the Clinger-Cohen Act did not call for the establishment of a federal CIO Council, the Administration is to be commended for taking the initiative to establish one through a July 1996 Executive Order.[24] Our experience with the CFO Act shows the importance of having a central advisory group to help promote the implementation of financial management reform. The CFO Council, which has a statutory underpinning, has played a lead role in creating goals for improving federal financial management practices, providing sound advice to OMB on revisions to executive branch guidance and policy, and building a professional community of governmentwide financial management expertise.

The CIO Council, chaired by OMB, can play a similarly useful role. As stated in its charter, the Council's vision is to be a resource for helping promote the efficient and effective use of agency information resources. The Council serves as the principle forum for agency CIOs to

- develop recommendations for governmentwide information technology management policies, procedures, and standards;
- share experiences, ideas, and promising practices for improving information technology management;
- promote cooperation in using information resources;
- address the federal government's hiring and professional development needs for information management; and
- make recommendations and provide advice to OMB and the agencies on the governmentwide strategic plan required under the PRA.

The CIO Council is currently going through a formative period. Since its first meeting in September 1996, the Council has engaged in a wide variety of activities. It meets on a monthly basis, bringing together CIOs, deputy CIOs, and representatives from major departments and agencies, as well as representatives from other organizations, such as the Small Agency

[24]Executive Order 13011 of July 16, 1996: "Federal Information Technology."

Council, the CFO Council, and the Governmentwide Information Technology Services Board.

The Council's activities during its first year have largely revolved around four major areas.

(1) *Council organization:* The Council decided how to organize and created operational procedures.

(2) *Committee specialization:* The Council created five committees to focus on selected topics of concern emerging from initial sessions—the year 2000, capital planning and investment, interoperability, information resources management training and education, and outreach/strategic planning. Each committee has pursued agendas that include regular working group sessions to exchange ideas and identify promising management practices.

(3) *Topical forums:* The Council has provided a regular forum for presentations and discussions of specific topics of shared concern, such as improving Internet security, enhancing the usefulness of budgetary reporting on federal information technology, understanding the use of governmentwide acquisition contracting mechanisms, developing effective systems architectures, and consolidating data center operations.

(4) *Governmentwide policy advice and recommendations:* The Council has responded to OMB's solicitation for comments on proposed federal information resources management policy revisions (the Federal Acquisition Regulations, Freedom of Information Act, the Privacy Act, the PRA); updates on critical issues such as Year 2000 progress; and guidance and feedback on agency reporting to meet OMB's federal oversight requirements (such as preparing budget submissions for information assets under OMB Circular A-11).

While these activities have proved useful, the Council does not yet have a strategic plan to help guide its work and serve as a benchmark for measuring progress. As we saw in the case of the CFO Council, achieving accomplishments that have strategic impact requires well-defined goals and measures. The CFO Council adopted a vision, goals, and strategies for financial management that have made it a much more productive body. The CFO Council now regularly reviews activities and, if necessary, revises Council priorities. In addition, the Council annually reports on its progress in implementing financial management reforms.

Recognizing the need to focus its efforts, the CIO Council began to reassess and redefine its strategic direction this past summer. This October, the Council members met at a day-long planning conference to discuss and finalize their long-range strategy. They agreed to focus their work on five strategic goals:

- establish sound capital planning and investment processes at the agencies;
- ensure the implementation of security practices that gain public confidence and protect government services, privacy, and sensitive and national security information;
- lead federal efforts to successfully implement the Year 2000 conversions;
- assist agencies in obtaining access to human resources with the requisite skills and competencies to develop, maintain, manage, and utilize information technology programs, projects, and systems; and
- define, communicate, and establish the major elements of a federal information architecture, in support of government missions, that is open and interoperable.

We believe that the CIO Council has selected the right set of issues to pursue. Several of these coincide with issues we raised in our 1997 High-Risk Series and recommendations we have formulated in conjunction with specific audit work. In addition, they parallel several concerns that the Congress—and this Subcommittee in particular—have raised about federal IT management. For example, the regular hearings and concerted effort by the Subcommittee on the Year 2000 computing crises have highlighted the urgency of the problem and helped to increase the attention and actions of federal executives. GAO has raised concerns about the pace at which federal agencies are moving to effectively address the Year 2000 problem.[25] In consonance with industry best practices, we have also developed and disseminated an assessment guide to help agencies plan, manage, and evaluate their Year 2000 programs, and are using this as a basis for selected agency audits.[26]

In addition, we have strongly recommended that agencies adopt a capital planning and investment-oriented approach to information technology decision-making.[27] It has been a key foundation for recommending

[25]Year 2000 Computing Crises: Time Is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997).

[26]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997).

[27]Information Technology: Best Practices Can Improve Performance and Produce Results (GAO/T-AIMD-96-46, February 26, 1996) and Information Management Reform: Effective Implementation Is Essential for Improving Federal Performance (GAO/T-AIMD-96-132, July 17, 1996).

improvements to the management of IRS' Tax Systems Modernization, HCFA's development of the Medicare Transaction System, and FAA's air traffic control modernization. We worked with OMB in 1995 to issue governmentwide guidance on information technology investment management[28] and we have also issued detailed guidance on how agencies can effectively implement an investment-oriented decision-making approach to their information technology spending decisions as expected under the Clinger-Cohen Act.[29]

Information security is also an issue of paramount importance to the information maintained and managed by the federal government. We have highlighted the reality of the government's vulnerability and the urgent need to effectively identify and address systemic information security weaknesses.[30] Moreover, in our September 1996 report on information security, we specifically recommended that the Council adopt information security as one of its top priorities.[31]

Also, building federal agencies' capability to manage information resources has been a critical problem for years. Several of our recent reports, for instance, have focused on serious weaknesses in an agency's capability to manage major technology initiatives, such as in the area of software acquisition or development.[32] Similarly, our best practices work has shown the importance of pursuing improvement efforts within the context of an information architecture in order to maximize the potential of information technology to support reengineered business processes.

We are encouraged by the Council's intention to establish a strong strategic focus for its work and further refine and prioritize the areas where it can best make a difference. One of the noteworthy aspects of the Council's goal-setting process was the members' desire to move away from

[28]Evaluating Information Technology Investments, A Practical Guide, Version 1.0 (OMB, November 1995).

[29]Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making, Version 1 (GAO/AIMD-10.1.13, February 1997).

[30]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996) and Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

[31]Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

[32]See, for example, Software Capability Evaluation: VA's Software Development Process Is Immature (GAO/AIMD-96-90, June 19, 1996); Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997; and Defense Financial Management: Immature Software Development Processes at Indianapolis Increase Risk (GAO/AIMD-97-41, June 6, 1997).

earlier draft language that defined the goals in terms of "promoting" and "supporting." Instead, the Council is working to frame specific, outcome-oriented goals. At the conclusion of the conference, the Council set up committees for each of the goals and charged them to decide on specific objectives and performance measures. The Council's aim is to complete this work quickly and publish its strategic plan in January 1998.

There is great urgency to deal with these major information technology problems. It is important that the Council demonstrate how CIOs are helping to make a difference by showing progress this coming year. GAO and OMB have given the CIO Council a head start by publishing guidance on information technology capital investments, information security, and best practices in information technology management.[33] By leveraging off this work, the Council should be able to build momentum quickly. Also, the CIO Council should follow the example set by the CFO Council, which publishes a joint report with OMB each year on its progress in meeting financial management goals. Having a visible yardstick will provide a strong incentive for both the Council and the agencies to make progress in meeting their information management goals and demonstrate positive impact on the agencies' bottom line performance.

Because it is essentially an advisory body, the CIO Council must rely on OMB's support to see that its recommendations are implemented through federal information management policies, procedures, and standards. In the coming months, the Congress should expect to see the CIO Council becoming very active in providing input to OMB on the goals it has chosen. OMB, in turn, should be expected to take the Council's recommendations and formulate appropriate information management polices and guidance to the agencies. There should be clear evidence that the CIO Council, OMB, and the individual CIOs are driving the implementation of information technology reforms at the agencies.

Ultimately, the successful implementation of information management reforms depends heavily upon the skills and performance of the entire CIO organization within departments and agencies—not just the CIO as a single individual. We have emphasized this point in our recent guidance on

[33]Evaluating Information Technology Investments: A Practical Guide, Version 1.0 (OMB, November 1995); Capital Programming Guide, Version 1.0 (OMB, July 1997); Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996); Business Process Reengineering Assessment Guide, Version 3 (GAO/AIMD-10.1.15, April 1997); and Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994).

information technology performance measurement.[34] With this in mind, we are working to produce an evaluation guide that offers a useful framework for assessing the effectiveness of CIO organizations. As with our other guidance, we intend to ground this approach in common management characteristics and techniques prevalent in leading private and public sector organizations. Using this methodology that focuses on both management processes and information technology spending results, we can provide the Congress and the agencies with in-depth evaluations of CIO organizational effectiveness.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you and members of the Subcommittee may have.

[34]Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments, Exposure Draft (GAO/AIMD-97-163, September 1997).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested