

**ESTABLISHING A FEDERAL CIO: INFORMATION
TECHNOLOGY MANAGEMENT AND ASSURANCE
WITHIN THE FEDERAL GOVERNMENT**

HEARING
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE
COMMITTEE ON
GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
SECOND SESSION

SEPTEMBER 12, 2000

Serial No. 106-261

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: <http://www.gpo.gov/congress/house>
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

74-562 DTP

WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512-1800 Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington,
MARK E. SOUDER, Indiana	DC
JOE SCARBOROUGH, Florida	CHAKA FATTAH, Pennsylvania
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
MARSHALL "MARK" SANFORD, South	DENNIS J. KUCINICH, Ohio
Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, Jr., Tennessee
GREG WALDEN, Oregon	JANICE D. SCHAKOWSKY, Illinois
DOUG OSE, California	-----
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont
HELEN CHENOWETH-HAGE, Idaho	(Independent)
DAVID VITTER, Louisiana	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

JAMES C. WILSON, *Chief Counsel*

ROBERT A. BRIGGS, *Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

BEN RITT, *Professional Staff Member*

BRYAN SISK, *Clerk*

TREY HENDERSON, *Minority Counsel*

CONTENTS

Hearing held on September 12, 2000	Page 1
Statement of:	
Atkinson, Robert D., director, technology & new economy project, Progressive Policy Institute	180
Doll, Otto, Commissioner, Bureau of Information & Technology, State of South Dakota, president, National Association of State Information Resources Executives	129
Flyzik, Jim, Deputy Assistant Secretary, Information Systems, Chief Information Officer, U.S. Department of the Treasury, vice chairman, Chief Information Officers Council	114
Ink, Dwight, president emeritus, Institute of Public Administration, former Assistant Director for Executive Management, Office of Management and Budget (1969–1973)	212
Katzen, Sally, Deputy Director for Management, Office of Management and Budget	6
McClure, David, Associate Director, Governmentwide and Defense Information Systems, U.S. General Accounting Office	17
Rummell, Paul E., president and chief executive officer, RLG Netperformance Inc., former chief information officer for the Government of Canada	173
Scherlis, William L., principal research scientist, School of Computer Science, Carnegie Mellon University	210
Letters, statements, etc., submitted for the record by:	
Atkinson, Robert D., director, technology & new economy project, Progressive Policy Institute, report entitled, “Digital Government, the Next Step to Reengineering the Federal Government,”	183
Doll, Otto, Commissioner, Bureau of Information & Technology, State of South Dakota, president, National Association of State Information Resources Executives, prepared statement of	132
Flyzik, Jim, Deputy Assistant Secretary, Information Systems, Chief Information Officer, U.S. Department of the Treasury, vice chairman, Chief Information Officers Council, prepared statement of	118
Ink, Dwight, president emeritus, Institute of Public Administration, former Assistant Director for Executive Management, Office of Management and Budget (1969–1973), prepared statement of	215
Katzen, Sally, Deputy Director for Management, Office of Management and Budget, prepared statement of	10
McClure, David, Associate Director, Governmentwide and Defense Information Systems, U.S. General Accounting Office, prepared statement of	19
Rummell, Paul E., president and chief executive officer, RLG Netperformance Inc., former chief information officer for the Government of Canada, prepared statement of	175

ESTABLISHING A FEDERAL CIO: INFORMATION TECHNOLOGY MANAGEMENT AND ASSURANCE WITHIN THE FEDERAL GOVERNMENT

TUESDAY, SEPTEMBER 12, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Davis, and Turner.

Staff present: J. Russell George, staff director/chief counsel; Randall Kaplan, counsel; Ben Ritt, professional staff member (GAO); Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong, staff assistant; George Fraser, intern; Trey Henderson, minority counsel; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

While we're having you all stand why don't we take the oath of office, as you know, for your testimony.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all of the witnesses have affirmed the oath.

I'll now make an opening statement, followed by the ranking member, the gentleman from Texas, Mr. Turner; and then we'll go down the line.

I might say to you what we said to the witnesses yesterday, you put wonderful statements in before us. We and the staff have had a chance to read it; and we're very grateful to you for—especially some of the ones that are out of town here. I think with the CIOs at the States that was very useful information. But we'd like you to summarize it in 5 minutes. Because what we want is a dialog here between the Members and between you. That way we get the best information out of it. So try to think about what are your key points after we start the opening statement.

Yesterday, this subcommittee examined the government's efforts to protect its computers and the sensitive information they contain. We heard testimony from the General Accounting Office that widespread deficiencies in computer security exists at a large number

of Federal departments and agencies. Some of the problems include poor implementation of policy and procedures and the lack of a coordinated security program among the departments and agencies.

Within recent memory two government agencies, the Federal Aviation Administration and the Internal Revenue Service, wasted more than \$7 billion on huge new computer systems that were ultimately scrapped because they could not deliver the services that it promised. Taxpayers cannot afford to have those management mistakes and the flagrant losses repeated.

We will examine two bills today that would establish a Federal Chief Information Officer and centralize management of the government's vast information resources: H.R. 4670, introduced by the subcommittee's ranking minority member, Representative Jim Turner of Texas; and H.R. 5024, introduced by subcommittee member Representative Tom Davis from Virginia.

I look forward to learning more about both proposals, and I'd like to welcome our witnesses today and look forward to their testimony.

I now yield time for an opening statement from the gentleman from Texas, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. I want to thank you for allowing us to have this hearing on this issue that I think is of utmost importance.

The information technology revolution of the last decade has had, as we all know, a profound impact on almost all aspects of our society. While the private sector has been quick to capitalize on the new opportunities created by the digital revolution, it is widely acknowledged that the Federal Government is behind the curve. The fact is, information technology offers as much to our government as it does to the private business. Among other advantages, it will allow us to literally put government at the fingertips of our citizens. A working e-government will mean that citizens can finally go online quickly and easily, instead of spending hours standing in long lines or waiting on hold to get the answers they need from government.

E-government can make government more customer friendly and, if we do it right, more cost-effective, saving millions of dollars for our taxpayers.

The information technology revolution also presents the Federal Government with one of the greatest management challenges we have ever seen. There is no doubt, however, that here in Washington we can mispend large amounts of money in incorrectly addressing the challenge. Just yesterday this subcommittee held a hearing on computer security, and numerous witnesses stressed the need to have cross-agency initiatives put in place rather than rely on each separate agency to duplicate the investment in finding solutions.

With the enactment of the Clinger-Cohen Act in 1996, all individual Federal agencies have a CIO, but the Federal Government as a whole does not. As the individuals responsible for providing information technology advice and policy recommendations, developing and facilitating information systems as well as evaluating and assessing those systems, the Federal Chief Information Officers play an essential role in fostering a digital government. The role of the

agency CIOs has been very positive. However, because of a lack of central authority and funding, there is little agency coordination when it comes to establishing crosscutting digital government applications.

We hear a lot today about the digital divide. In the Federal Government there is a different kind of digital divide where each separate agency pursues the application of information technology without the benefit of significant government wide leadership.

In an effort to close the Federal Government's digital divide I've introduced H.R. 4670, which would create a framework for a Federal Chief Information Officer located in the Executive Office of the President. The position would report directly to the President and direct the process of developing an aggressive digital government conversion plan. He or she would have a small staff and a budget independent of individual agencies to help drive the next generation of digital government, much of it involving cross-agency applications.

The Federal CIO would also take the lead in shaping the administration's policy regarding the Internet and computer security. The Federal CIO would select the best ideas for e-government, develop pilot programs and test them in selected agencies and establish priorities for the application of information technology to improve government. The Federal CIO would be the lead coordinator to forge stronger digital partnerships with State and local governments.

I commend the chairman for having this hearing; and I commend my colleague, Tom Davis of Virginia, who has introduced his own bill on this topic.

I realize that there are issues surrounding where the Federal CIO will be located and what specific statutory authority he or she may be given. This discussion requires careful consideration of the current statutory responsibility of the Office of Management and Budget and an analysis of the current role of the OMB's Deputy Director for Management, who's here today. We appreciate the good work and input that Ms. Katzen has given us and OMB's Office of Information and Regulatory Affairs.

OMB's budget and oversight role over all executive functions clearly includes information technology, and it is not my intent to fail to acknowledge the fine work the office has done. Rather, with this legislation I seek to enhance the capability for leadership and the effective and timely application of information technology to government.

There are several points that I believe are essential to the success of a Federal CIO. These include a high-profile leadership role to elevate the visibility and focus of information technology and who reports directly to the President.

Second, the establishment of a good working relationship with OMB and the Federal agency CIOs.

And, third, direct access to funds to ensure the capability to carry out meaningful initiatives.

This hearing affords the first opportunity in this Congress to consider the concept of a Federal CIO. Both Presidential candidates have publicly expressed their support for a new position with a defined focus on e-government. This is clearly an idea whose time has come. It is my hope that this hearing will move us forward on this

idea, solidify our resolve to maximize the potential of information technology in government and more clearly define the structure that this position should take to maximize its effectiveness.

In government, we have a clear need to meet the challenge of the digital age. It is not just a matter of resolving conflict; it is a question of whether or not we will take advantage of the phenomenal growth of information technology, whether we will make dot-gov as commonplace as dot-com.

Again, I commend the chairman for the opportunity to have this hearing, and I look forward to hearing from each of our witnesses.

Mr. HORN. I thank the gentleman and now yield opening time for the gentleman from Virginia, Mr. Davis, who has another proposal in this area; and I'd like him to expand on that now.

Mr. DAVIS. Thank you. Mr. Chairman, I want to, first, thank you for your responsiveness in holding this hearing today to examine the merits of establishing a Chief Information Officer for the Federal Government based on proposals introduced by both myself and my colleague Mr. Turner.

I also want to express my deep appreciation to our ranking member for his foresight in focusing on an issue which I believe is critical to improving the ability of government to be an efficient user, coordinator, manager, disseminator and protector of information resources, particularly with respect to information technology.

I'll spend my few minutes highlighting the dominant themes which shaped my proposal, the Federal Information Policy Act, to create a Federal CIO who is vested with the primary authority to coordinate information resources management within and amongst all Federal agencies, including the implementation of effective, mandatory controls over government information security through a new Director of Information Security and Technical Protection.

A decade ago, technology stood as one of many factors important to the mission and performance objectives of the Federal Government. But no longer is technology one of many. Instead, the Information Revolution and the ever-evolving technologies that support its collection, assimilation and communication have become integral to the functioning of our government. The past 5 years alone are testimony to a remarkably fast-paced change in the ability of Americans to communicate and access information through the personal computer and the Internet.

It's the responsibility of the Federal Government to adapt its institutional processes of the old age to the new economy and become a national model for information resources management and information security practices through the acquisition and use of information technology.

The current processes appear to lack a focused, coordinating body to implement effective IRM policies and develop a common strategy for interagency efficiency and cooperation. Although the Office of Management and Budget has responsibility for information resources management governmentwide, I'm deeply concerned that OMB, through the Office of Information Regulatory Affairs, is simply unable to devote the attention needed for carrying out effective information resources management as directed under current law. For instance, in July 1998, the General Accounting Office [GAO], examined two of the IRM-related responsibilities assigned to OMB

in the Paperwork Reduction Act and delegated to OIRA but found that OIRA had not satisfied either of them. Those responsibilities were developing a governmentwide IRM plan and periodically reviewing a selected agency's IRM activities. And last year the GAO found that improvements in broad IT management reforms will be difficult to achieve without effective agency leadership, highly qualified and experienced CIOs and effective OMB leadership and oversight.

If we can't get the management of our information resources in order, how are we ever going to be able to implement the electronic government initiatives supported by this subcommittee and the Congress, as well as by the administration, that will allow American citizens to communicate more easily with their government?

A critical component of protecting information resources is the governmentwide coordination and implementation of proven information security practices. Currently, responsibility for overseeing computer security procedures and reviews is handled by a number of agencies including OMB, the National Institute of Standards and Technology, the General Services Administration, and the National Security Agency. Notwithstanding the number of agencies involved in various aspects of information security, there is an abundance of evidence highlighting the vulnerabilities of Federal computer systems in both internal and external intrusions.

First and foremost is the portrait that emerged as a result of the subcommittee's hearing yesterday in computer security in which the Federal Government received an overall grade of D minus. As well, at a March 29th hearing, GAO cited earlier findings that 22 of the largest Federal agencies were providing inadequate protection for critical Federal operations and assets from computer-based attacks. GAO reported that within the past year it was able to identify systemic weaknesses in the information security practices of the Department of Defense, the National Aeronautics and Space Administration, Department of State, and the Department of Veterans Affairs. In each instance sensitive data and/or mission-critical systems were penetrated by unauthorized users.

In early August, the Washington Post reported that the State Department had to warn its employees about downloading large MP3 sound files on their workstations and the, "adverse effect on the networks as these files enter the e-mail system." Part of the best information security practices is endowing your employees with the necessary awareness of methods for security intrusions, such as downloading unknown files and introducing them into a computer network.

Two days later, in discussing the persistent threat of computer hackers to the Department of Defense, the Washington Post reported that it is highly—it was highly probable that at least some of the 22,000 attacks last year were mounted by foreigners probing U.S. security gaps. These facts alone prompt serious concerns about the integrity of the most basic access controls for Federal information systems.

Mr. Turner and I have established a strong basis for working together with the members of the subcommittee, the administration, and the private sector to secure the ability of our Federal Government to better manage its information resources and fully utilize

information technology to better serve American citizens. Our legislation is similar in that each bill gives the CIO top-level authority and direct access to the President and also codifies the CIO Council.

While Mr. Turner's bill envisions the Federal CIO as acting as an advisor, resource and visionary for information technology management, my legislation goes several steps beyond and further encompasses all the information resources management functions that rely on IT and which are critical to building a government that can serve its citizens in a digitally driven world.

The Federal Government is fast falling behind the curve, and I strongly believe that establishing an empowered CIO is essential to achieving that goal.

I want to welcome our panel of witnesses today and look forward to hearing their perspectives and suggestions for succeeding in making the Federal Government a leader and innovator in the management, promotion and protection of government information systems. Thank you.

Mr. HORN. We thank you.

We now move toward our witnesses.

The first witness will be the Honorable Sally Katzen, the Deputy Director for Management, Office of Management and Budget. We'll give the administration 2 extra minutes as a matter of reciprocity and curtesy. So we're glad to see you here.

**STATEMENT OF SALLY KATZEN, DEPUTY DIRECTOR FOR
MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET**

Ms. KATZEN. I'm glad to be here. I'm delighted to be here. I have waited a long time for the opportunity to return to testify before you and, as in the past, you've picked a great issue to focus on.

As Mr. Turner noted, there is no doubt that IT plays a fundamental role in our endeavor to create a government that's more accessible and more responsive to the public. Nor is there any doubt about the other types of advantages that IT can bring. It can also bring significant challenges such as security and privacy and accessibility.

So today the questions of how to manage and fund Federal information technology enterprise are among the most critical facing Federal managers. And unlike the Y2K problem, which is the background for suggestions, from some people at least, about a Federal CIO, dimensions of information policy and technology oversight responsibilities are ever-expanding and involve every aspect of the government's operations—or at least they should involve every aspect of the government's operations.

Now in my written testimony I devote many pages to the administration's record of managing the IT effort, and I won't repeat that here. I do want to make three observations.

One, while we do not have someone with the title Federal CIO, many if not all of the responsibilities identified have been carried out through OMB, through the Office of the DDM, through the Office of the Administrator of the Office of Information and Regulatory Affairs; and I think we've done a very good job.

Over the last 7½ years, we—with support from the President and the Vice President, we have focused on what have been the

most important issues at the time. The early part of the decade we were focusing on systems, and the FAA and the IRS that the chairman cited have been turned around as we focus on customer off-the-shelf types of things, modular development, "Raines rules" that we have been using.

We then turned our attention, as this subcommittee well knows, to Y2K. And despite initial concerns that we would never meet the date change and some very bad grades on report cards, we were highly successful in that effort with your help and with the help of others.

And, finally, we have turned in the last year to focus on some of the other issues, the paramount one being e-government but also computer security. Capital planning, data sharing are subjects which we will probably come up with.

The second point is while I think we have been very successful we have done a lousy job of communicating how much progress we've made. People are often surprised when they make a suggestion and learn we're already doing it. I listen to some of the things that have been cited as we need to do and I think to myself, we are doing it. We're just not being very effective in telling people about it. Whether it's management tools like sharing savings, whether it's spacial types of data, the FirstGov, the digital signatures, and indeed the CIO Council, which you'll hear more from Mr. Flyzik, every agency is not reinventing the wheel. We have an effective forum for sharing best practices and carrying forward. We are not doing a very good job of telling people about it.

And the third point that I'd like to make is that our success is due not only to leadership from the top, and I'm referring here to the President and Vice President, and from leadership from the Congress, and your committee has been outstanding in that regard, but also because of the hard work of the many people at the agencies and their leaders who understand how IT fits into their mission and programs to provide a better and more effective government. This was a salient fact of Clinger-Cohen which gave the agency head responsibility for investment decisions of IT because they know how IT fits with their missions.

Now, with respect to the subject of this hearing, everybody agrees on the importance of promoting and managing Federal IT; and everyone agrees that there should be a higher level of visibility and a more enhanced effort. There are different views about how to get the job done.

As the chairman mentioned, one that has some currency now is to enact legislation that would create a new Federal CIO. As my testimony indicates, I think the real questions go to what the leaders of the Federal IT enterprise should do and how they should do it.

I thought Mr. Turner asked all the right questions. I hope we'll have a chance later to start explaining what it is that we are doing in that area.

But because IT is integral to every operation of government, we think IT leadership must be part and parcel of the government's budget and program decisionmaking process. In other words, the strategic management of Federal IT resources should not be separated from other management and budget concerns. It must be in-

tegrated. It is imperative, we believe, that officials with accountability for IT have direct influence over the spending and execution of IT investments.

Severing the tie between responsibility for oversight of IT and budgeting for IT would undermine both and retard the progress that both the Congress and the executive branch recognize as essential. Indeed, separating the Office of Management and Budget from the management and budgeting for Federal IT is like taking the oranges out of orange juice. What's left is drinkable, but it's neither tasty nor nutritious. OMB's strength is its governmentwide authority, combined with expertise in individual agency mission budgets and programs. We set policy governmentwide and oversee implementation on a case-by-case basis. This is our strength. We are urged to play our strength.

I cannot emphasize enough how important this function is at OMB. The OMB Director devotes significant time to IT management issues, and his leadership has energized our efforts. OMB also deals with critical information policy issues such as access dissemination in FOIA as well as computer security and privacy. The DDM manages these efforts both within OMB and across the government.

The DDM has strong support from the OIRA administrator. As a former Administrator of OIRA, I can tell you how important and significant a component that is. Now we recognize there could well be enhanced efforts for OMB to promote and lead agency IT efforts. We have started this effort, and we welcome a dialog with this committee and with others here at the table as to what we should be doing to improve our efforts.

Mr. Chairman, as I noted in my testimony at the end, I offer these views based on 6 years experience of managing information technology in the Federal Government but also in recognition that we're only 2 months before an election and 5 months before a transition to a new President. As Mr. Turner mentioned, both major candidates have made Federal IT an important program in their agendas and both share your goal and ours of continually looking at ways to improve Federal IT management.

The two bills you've asked me to comment on both speak to what is essentially a management issue: How to organize oversight of the government's most important function. And I suggest that legislation now would only tie the new President's hands. We ought to give the new administration an opportunity to consider the approaches in these two bills and other approaches to IT and management and give us their recommendations before any action is taken.

Again, I join those who recognize and applaud this committee's interest in how government manages and uses IT. We think that hearings such as this are extraordinarily helpful to keep us all focused on how best to achieve those goals. We have full confidence that this partnership will ensure that the next administration can build on our progress to deliver the American people the quality of

government they expect.

Thank you very much, Mr. Chairman.

Mr. HORN. We thank you for your diligence and are glad to see you back doing all this.

[The prepared statement of Ms. Katzen follows:]



DEPUTY DIRECTOR
FOR MANAGEMENT

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF THE HONORABLE SALLY KATZEN
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
September 12, 2000

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to share my views on how best to lead the government's information technology enterprise. We welcome your interest and more importantly your leadership in this area, and the opportunity to begin working with you on these very important issues.

OMB shares this Subcommittee's interest in taking full advantage of information technology (IT) to improve government. There is no doubt that IT plays a fundamental role in our endeavor to create a government that is more accessible and more responsive to the public. Nor is there any doubt of the advantages that IT can bring. It can also bring significant challenges, such as privacy, security, and accessibility.

Today, information technology is one of the most critical issues facing Federal managers. Unlike the Year 2000 problem, dimensions of information policy and technology oversight responsibilities are ever-expanding and involve every aspect of the government's operation. The Office of Management and Budget is working hard to ensure that agencies deliver results in this area. The Clinger-Cohen Act places the responsibility for managing information technology investments on agency heads. At the same time it provides for centralized leadership by giving OMB the responsibility to improve the acquisition, use, and disposal of information technology by the Federal government in order to improve the productivity, efficiency, and effectiveness of Federal programs. Clinger-Cohen authority is implemented through the Deputy Director of Management (DDM), who also chairs the CIO Council.

Your letter of invitation raises questions about various proposals to create a Federal Chief Information Officer (CIO), such as whether there should be a Federal CIO, where the CIO should reside, and how the CIO would be empowered. The letter also asks for our views on two proposed bills, H.R. 5024 and H.R. 4670, both of which would create a Federal CIO in different ways. I would like to put our views on the issues you have raised in context, by first describing how this Administration has exercised leadership in information technology, and then what those experiences teach us about future management challenges.

The Administration's Record of IT Leadership

The President and the Vice President have repeatedly emphasized the importance of IT in creating a government that is more accessible and responsive to citizens. Our early efforts in this Administration focused on the management of specific agency systems. Historically, Federal agency systems were custom built, frequently came in over budget, and were so delayed as to be almost obsolete by the time they were fully implemented. We changed this by emphasizing off the shelf technology, open architecture, and modular development. We began to see dramatically improved results. Our efforts were enhanced by the passage of the Clinger-Cohen Act, where we worked with the Congress on a bipartisan, bicameral basis.

To aid agency implementation of Clinger-Cohen, former OMB Director Frank Raines issued an OMB Memorandum titled "Funding Information Systems Investments," commonly referred to as "Raines' Rules". This Memorandum established the decision criteria OMB uses to evaluate all major information system investments proposed in the President's budget. These rules initiated fundamental change in the management of Federal IT management.

As this Subcommittee well knows, over the next few years we focused on the Year 2000 problem. This involved a massive government-wide push to meet, and ultimately beat, the date change. The work was done by thousands of dedicated Federal employees and contractors, with OMB responsible for overseeing Federal systems. The Y2K Council vigorously engaged in outreach to state, local, and tribal governments, as well as the private sector, both domestic and international. The Chair of the Y2K Council was John Koskinen -- not a CIO, but rather someone who had just stepped down as DDM of OMB.

In the last year, we have shifted our focus to a number of other important IT initiatives which are included in the President's FY2001 budget as priority management objectives (PMOs). Over the past several years, OMB has identified significant management challenges that warranted senior level attention as PMOs. The current PMOs that focus on the management of information technology and policy include strengthening capital planning, improving computer security, expanding data sharing, and promoting electronic government.

The PMO for capital planning manages and reports on the health of the government's IT portfolio by focusing on improving acquisition and use of information systems across the government. Capital planning and investment control allow agencies to plan, budget, and execute IT investments in a way that contributes to the agency's missions and accounts for risks, benefits, and costs throughout the life of the investments. In the last year, we have made much progress in this area by partnering with the agencies, assessing their processes, and providing specific feedback throughout the budget process to ensure that the information technology investments are tied to mission objectives and achieve their cost, schedule and performance goals. Although the implementation of Clinger-Cohen continues to be uneven across the agencies, we are working with the agencies using this framework and the overall IT portfolio to better manage information technology in the Federal government -- and we are seeing real results.

You heard yesterday about computer security from the OIRA Administrator, John Spotila. The PMO for computer security and critical infrastructure focuses on the reliance on

computer systems to support critical functions. In order to enhance the security of Federal information systems and critical infrastructures, we need to counter risks to increasingly interconnected computer networks in government and critical industry sectors. We have a number of projects under way to accomplish this goal. For example, OMB is currently assessing agency responses to a questionnaire on the security of systems that support the 43 high-impact programs. We will highlight for agencies the areas of concern, and will work within OMB and the agencies to correct deficiencies.

Through the PMO on data sharing, we are working to encourage that the right person gets the right benefit. We encourage agencies to first determine whether they have significant erroneous payments and, if so, to then use data sharing opportunities to reduce those erroneous payments -- ideally up-front before they are disbursed. Our efforts here also focus on ensuring that proper privacy and security safeguards are in place in data sharing programs. As agencies increase electronic information collection pursuant to the Government Paperwork Elimination Act and other programs, there are more opportunities to engage in data sharing via automated computer matches.

Another PMO, "Implementing Electronic Government," is a major priority for OMB. Electronic government offers a unique opportunity to improve the way we govern. It has the potential to affect virtually every Federal activity. Success will require leadership and coordination across the Federal government.

Electronic Government

To accelerate and focus the Federal government's work, last December the President issued a Memorandum to the Heads of Executive Department and Agencies regarding Electronic Government. The Memorandum calls for a number of actions, including:

1. Establishing a "one-stop" gateway to government information available on the Internet. The information will be organized by the type of service or information that people are seeking, rather than by agency. This effort is called FirstGov.gov and I will return to it later in the testimony.
2. Identifying forms for the top 500 Government services used by the public and making them available online this year.
3. Implementing the Government Paperwork Elimination Act by gathering and making information available electronically.
4. Building good privacy practices into Federal web sites.
5. Creating public email addresses for citizens to contact agencies.
6. Ensuring accessibility for the disabled.
7. Using the web to improve procurement.
8. Fostering the use of digital signatures by agencies and the public, with at least 100,000 issued this year.
9. Developing a strategy for Internet use that enables agencies to become more open, efficient, and responsive, so they may carry out their missions more effectively.

As DDM, I chair the President's Management Council (PMC), which is comprised of the Chief Operating Officers from the major Departments and agencies. The PMC adopted as one of its three goals for the year 2000 "Promoting Electronic Government," and it has adopted four priorities that build upon the President's Memorandum:

1. The placement of forms and other information online under a single access point (FirstGov);
2. The development of customer-centric web sites for specific purposes like exports and procurement;
3. The widespread use of digital signatures; and
4. The adoption of at least one electronic government process in every agency.

In addition, in leading the transition to electronic government, OMB has organized the many interagency efforts that have evolved to promote e-gov. We do not want to stifle any initiatives but we also do not want to duplicate efforts. For that reason, each interagency effort is to be undertaken under the auspices of an existing management council, including the Chief Information Officers' Council (CIOC), the Chief Financial Officer's Council (CFOC), and the Procurement Executive Council (PEC). As DDM, I chair monthly meetings of representatives from these councils, sorting through proposed e-government initiatives, coordinating interagency efforts, and setting priorities when necessary.

Furthermore, on May 2, 2000, OMB issued guidance for implementing the Government Paperwork Elimination Act (GPEA), another example of successful collaboration on legislation between the Executive and Legislative Branch. The guidance will help agencies remove barriers to interacting electronically with citizens. It addresses electronic signatures, system security, risk management, and privacy. In addition, Treasury, Commerce, NARA, and Justice are issuing topic specific agency guidance under GPEA. As you know, GPEA requires Federal agencies to allow individuals or entities that deal with the government the option of submitting information or transacting with the agency electronically, when practicable, by October of 2003. We are leading agency work to meet that deadline.

While we have made much progress in many of these areas, let me focus on two that bring transformational change: firstgov.gov and the development of an interoperable Public Key Infrastructure (PKI).

FirstGov.gov

Over the coming months, the Administration is going to provide the public a single, citizen-focused web site, where they can find every on-line resource offered by the Federal government at one easy-to-use location. The FirstGov web site, www.firstgov.gov, will have the ability to search half a billion documents in less than one-quarter of a second, and will be able to handle up to millions of searches a day. It will not only make it much faster and easier for citizens to find the government information and services they are looking for, they can also do it at anytime – 24 hours a day, 7 days a week. This could mean an end to waiting in lines or on the phone. Additionally, the site will safeguard citizen's communications and transactions with the

government, protect their privacy, and will leverage a partnership with the private sector to maximize innovation and usability.

Access to government information will be organized by type of service or topic, and will contain single, government-wide points of entry developed for selected topics. For example, over the coming year the Administration will make it possible for people to go online at FirstGov and quickly learn about the vast majority of procurements and grant opportunities through a simple online process. Through FirstGov, citizens will have easy access to sites that let you apply for student loans, find new jobs, find the latest health research, and do much, much more.

Public Key Infrastructure (PKI)

A second key example of our work to facilitate electronic government is in the development of a Public Key Infrastructure so that citizens can conduct business with the government through a private and secure electronic transaction path. The General Services Administration, in coordination with the Department of the Treasury, the Department of Commerce, and the Chief Information Officers' Council, is leading the effort under OMB oversight. This is accomplished using PKI-based digital signatures from GSA's "Access Certificates for Electronic Services" (ACES at www.gsa.gov/aces), and building an interoperable framework to accept signatures under the Federal Bridge Certification Authority (see gits-sec.treas.gov). Over the next four months, the GSA Administrator will issue up to 500,000 digital signatures enabling secure communication with the government—well above the 100,000 goal in the Presidential directive. However, this goal is critically dependent on funding, and the Administration's requested funding of \$7 million for public key infrastructure in the FY 2001 budget faces uncertain prospects for final passage.

Should we legislate a "Federal CIO?"

Everyone agrees on the importance of promoting and managing Federal IT, but there are apparently different views as to how best to do the job. One idea that has some currency now is to enact legislation that would create a new "Federal CIO". The suggestion has been raised several times in different contexts. Several years ago we discussed this issue with Congress as we worked on the Clinger-Cohen Act. At that time, Congress and the Administration agreed that the Director of OMB, working with agency heads, should be charged with these responsibilities. Executive Order 13011 reinforced this authority, creating the CIO Council under the leadership of the Deputy Director for Management. The suggestion came up again in the context of Y2K. In that instance, the President chose to create, by Executive Order, a council chaired a former OMB DDM, to focus on the single task of ensuring the country was ready for the date change.

More recently, on April 7, 2000, OMB Director Jack Lew spoke before this Subcommittee on this subject. There was a long colloquy during which he reiterated the Administration's views. He noted that the history and the future of IT have always been about change -- we cannot just build it once and say "We are done." We must have an active, ongoing IT investment process, one that is institutionalized, flows from an agency's mission, and is an essential part of its budget formulation and execution. He added that strategic management of

Federal IT resources should not be separated from other management and budget concerns -- it must be integrated. It is thus imperative that officials with accountability for IT have direct influence over the spending and execution of IT investments. Severing the tie between responsibility for oversight of IT and budgeting for IT would undermine both, and it would retard the progress that both the Congress and the executive branch recognize is essential. Indeed, to separate IT leadership from OMB is to weaken the entire government's ability to get our hands on the problem. In our view therefore, the right answer is to strengthen how we use the existing authority and leadership responsibilities of OMB. The Director also testified that if the perception is that OMB has not done enough, then we ought to solve the problem by stepping up our efforts, which we have done.

These were the views of the Director of OMB in April of 2000, and these are my views today. I believe that in the first instance agencies must manage IT investments consistent with their missions and programs. For this reason, Clinger-Cohen is correct to require the head of each agency to be responsible for the management of information technology investments. I also believe that there is an important role for centralized leadership, and therefore again Clinger-Cohen is correct in placing these responsibilities with OMB. OMB has budget and program oversight responsibilities throughout the Executive branch and can work to ensure that IT supports agency missions and policies. In addition, as DDM I chair the PMC Council as well as the other Councils (Chief Information Officers Council, Chief Financial Officers, Procurement Executive Council, etc.) that deal with management issues within the agencies. Successful oversight of IT must include authority to control resource allocations and management direction. OMB has all of this.

The OMB Director devotes significant time to IT management issues, and his leadership has energized our efforts. In addition to the management issues I previously described, OMB deals with critical information policy and technology issues, such as access, dissemination, and FOIA, as well as computer security and privacy. The DDM manages these many efforts both within OMB and across the government. The DDM also has strong support from the OIRA Administrator, who has statutory responsibility for computer security and monitors management of agency IT systems and IT spending. OIRA also staffed OMB's oversight of the government wide Y2K effort. As a former Administrator of OIRA, I can confirm that IT is a significant component of that position.

As the Director noted in his testimony, we recognize that there could well be enhanced efforts by OMB to promote and lead agency IT initiatives. We have started this effort and welcome a dialogue with you on how to improve our efforts.

Finally, you asked for comment on two bills that would seek to assign management responsibilities for Federal IT to a Federal CIO. Both bills also would establish Federal CIO offices within the Executive Office of the President -- but outside of OMB. H.R. 4670 would create a small office modeled after the Y2K office, while H.R. 5024 would create a larger office that would assume many of the functions currently performed by OMB. As I have said, we believe that separating oversight of IT management from OMB's management and budgeting authority will not achieve integrated and coordinated results, but rather will have negative effects on both IT, budgeting for IT, and programs enabled by IT.

Interestingly, in response to the idea of a Federal CIO as outlined on the Electronic Government web site hosted by Senators Thompson and Lieberman, and in early reactions to the bills currently introduced in the House of Representatives, the majority of agencies -- while in favor of strengthening existing structures -- opposed creating a new position outside the existing structure for IT oversight. Indeed, some agencies believe that measures to strengthen the role and effectiveness of individual CIOs within Departments is more appropriate than creating a new Federal CIO with broad decision-making responsibilities.

Mr. Chairman, I offer these views based on over six years experience managing information technology in the Federal government, but also in recognition that we are only two months before an election and five months from the transition to a new President. Both major candidates have made IT an important program in their agendas, and both share your goal and ours of continually looking at ways to improve Federal IT management. The two bills you asked me to comment on both speak to what is essentially a management issue -- how best to organize oversight of one of the government's most important functions. Legislation now would tie the new President's hands. While consideration of this issue now may be helpful, the next Administration should have the opportunity to consider the approaches in these bills and other approaches to IT policy and management before any action is taken.

Moreover, it may be that legislation is not necessary. As I mentioned, we were very successful with the Y2K effort without any statutory office being created. Indeed, with technology changing so rapidly, legislation that mandates a particular approach may lock in oversight structures and constrain our capacity to solve problems that are unknown to us today. Thus while much work remains in this area, and while legislating a Federal CIO may seem like a panacea to some now, it is not necessarily the right answer.

We recognize and applaud the Committee's interest in how the government manages and uses IT. We think that hearings such as this one help to keep all of us focused on how best to advance the goals we both share. And we have full confidence that this partnership will ensure that the next administration can build on our progress to deliver to the American people the quality of government they expect and deserve.

Thank you and I look forward to answering any questions.

Mr. HORN. David McClure is the Associate Director, Governmentwide and Defense Information Systems for the U.S. General Accounting Office, part of the legislative branch. Mr. McClure.

STATEMENT OF DAVID McCLURE, ASSOCIATE DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE

Mr. McCLURE. Good morning Mr. Chairman. Mr. Turner, Mr. Davis, pleasure to be here.

I really want to cover three crucial points concerning this topic of the Federal CIO this morning and expand on them briefly.

First, I think sustained and focused central leadership for information technology management is essential for the Federal Government. It should enhance and not constrain similar IT leadership and accountability in the Federal agencies.

Second, the form and the structure of the CIO position should follow closely to the functions that you expect the office to perform.

And, third, the two legislative proposals before the Congress offer two distinctively different approaches for elevating the visibility and focus of Federal information management and technology. Each proposal has its benefits, but each also will face implementation challenges.

Let me expand on each of these points briefly.

First is the need for established and focused central leadership. Increasingly, Federal information management and technology challenges are multidimensional, and they're horizontal in nature. They cut across traditional program and agency lines.

As noted in the report that we're issuing today to you, Mr. Chairman, on management lessons learned from Y2K, a Federal CIO could be instrumental in focusing on actions that go beyond those traditional boundaries. This necessitates governmentwide oversight, interagency collaboration and funding, and cooperation with State governments, local governments, and the private sector.

Today's critical IT issues, including IT management issues, security, critical infrastructure protection, electronic government, and IT human capital really all require tightly focused, constant governmentwide leadership and direction. It's for that reason we support the creation of a Federal CIO today, just as we did during the deliberations of the Clinger-Cohen Act in 1995.

Agency leaders and agency CIOs should be held accountable for their IT missions within their own agencies. But a Federal CIO can bring a lot to the table. He or she could identify and set the agenda for governmentwide policy issues needing attention; he or she could focus on established priorities in ensuring that related efforts are complementary rather than duplicative of each other; and the national CIO could direct the attention and resources to consolidating interagency governmentwide process through shared information technology assets.

My second point relates to the critical need for the Federal CIO position to be structured for success. We've done research on successful CIOs in both the public and the private sector. The trend for these positions is—especially in the government—is for the CIOs to have governmentwide responsibilities. In creating this position there are two critical success factors that are paramount:

First, top level political support and attention to IT management; and, second, clear roles, responsibilities, accountabilities and sufficient stature to maximize CIO impact and success.

My third point involves the distinctively different models for a Federal CIO presented by these two legislative proposals. Let me point out, however, that they do have similarities. For example, they both make the Federal CIO a Presidential appointee who reports directly to the President with cabinet level status. The high visibility afforded to this position should not be underestimated. It is a clear critical success factor for all CIOs in any organizations. Both bills also leave intact OMB's role and responsibility to review and ultimately approve agencies' budgets for inclusion in the President's submission.

Additionally, both bills establish the CIO Council and statute and we believe there are tremendous benefits in doing so.

The chief differences between these two bills lie mainly with the scope, the role, the responsibilities of the CIO. Mr. Davis' bill vests the Federal CIO with policy guidance and oversight responsibilities that currently reside with OMB. This would create a single central focus for information, management and technology. And the multitude of the duties associated with the DDM position in OMB and the regulatory burden and paperwork reduction performed by OIRA really limit the ability of OMB to provide full-time focus and attention to the government's pressing IT problems.

So to sum up, let me reiterate a point that is made in Ms. Katzen's written statement. There is clearly no consensus if the Federal community on the need for a Federal CIO. I think that can be attributable to the uncertainty about the details regarding how the position would be created, its role, its authority, its responsibility. Still we believe there's a clear need for focused central leadership to increase the government's ability to use information resources at its disposal effectively, securely and with the best service to the American people.

Thank you, Mr. Chairman.

[The prepared statement of Mr. McClure follows:]

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. EDT
Tuesday,
September 12, 2000

**FEDERAL CHIEF
INFORMATION OFFICER**

**Leadership Needed to
Confront Serious
Challenges and Emerging
Issues**

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



GAO/T-AIMD-00-316

Mr. Chairman and Members of the Subcommittee:

It is a pleasure to be here to participate in today's hearing on establishing a federal chief information officer (CIO). As you know, the rapid pace of technological change and innovation has offered unprecedented opportunities for both the government and commercial sectors to use information technology (IT) to improve operational performance, reduce costs, and enhance service responsiveness to citizens and consumers. Yet at the same time, a range of issues have emerged about how to best manage and integrate complex information technologies and management processes so that they are aligned with mission goals, strategies and objectives.

In 1999 we issued a series of reports—our Performance and Accountability Series—that describe management challenges confronting individual agencies and the government as a whole.¹ One of the many challenges facing the government is effectively using information technology to help achieve program results. Since 1990, we have also periodically reported on government operations that we have assessed as high risk because of their greater vulnerability to waste, fraud, abuse, or mismanagement. In the information resources and technology management area, we have designated information security² and four agency IT modernization efforts as high risk.³

The government has made improvements in its IT management, such as updating policies and guidance to reflect best practices. Moreover, agencies are responding with concerted actions to effectively address critical IT management shortcomings. Nevertheless, our work shows that agencies continue to be challenged by (1) fundamental weaknesses in information technology investment selection and management control processes, (2) slow progress in designing and implementing information technology architectures, (3) inadequate or immature software development, cost estimating, and systems acquisition practices, (4) the need to build effective chief information officer leadership and organizations, and (5) significant computer security weaknesses.

¹*Major Management Challenges and Program Risks: An Executive Summary* (GAO/OCG-99-ES, February 1999) provides an overview of this series.

²Beginning in 1997, we also designated the Year 2000 computing challenge as a high-risk area.

³*High-Risk Series: An Overview* (GAO/HR-95-1, February 1995), *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February, 1997), and *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

Sustained and focused central leadership is key to improving the federal IT performance track record. Two legislative proposals for helping achieve such leadership have been introduced by members of this Subcommittee—H.R. 4670, the Chief Information Officer of the United States Act of 2000, introduced by Representative Turner; and H.R. 5024, the Federal Information Policy Act of 2000, introduced by Representative Davis.

In my remarks today, I will

- briefly describe the background of the federal government's current information resources and technology management framework,
- briefly explain the structure and responsibilities of existing state and foreign governmentwide CIO models,
- discuss the federal CIO approaches proposed by the two bills, and
- discuss the type of leadership responsibilities that we believe a federal CIO should possess.

Background

The federal government's information resources and technology management structure has its foundation in six laws: the Federal Records Act, the Privacy Act of 1974, the Computer Security Act of 1987, the Paperwork Reduction Act of 1995,⁴ the Clinger-Cohen Act of 1996, and the Government Paperwork Elimination Act of 1998. Taken together, these laws largely lay out the information resources and technology management responsibilities of the Office of Management and Budget (OMB), federal agencies, and other entities, such as the National Institute of Standards and Technology.

In general, under the government's current legislative framework, OMB is responsible for providing direction on governmentwide information resources and technology management and overseeing agency activities in these areas, including analyzing major agency information technology investments. Among OMB's responsibilities are

- ensuring agency integration of information resources management plans, program plans, and budgets for acquisition and use of information

⁴The Paperwork Reduction Act of 1995 revised the information resources management responsibilities established under the Paperwork Reduction Act of 1980, as amended in 1986.

technology and the efficiency and effectiveness of interagency information technology initiatives;

- developing, as part of the budget process, a mechanism for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems;⁵
- directing and overseeing implementation of policy, principles, standards, and guidelines for the dissemination of and access to public information;
- encouraging agency heads to develop and use best practices in information technology acquisition;
- reviewing proposed agency information collections to minimize information collection burdens and maximize information utility and benefit; and
- developing and overseeing implementation of privacy and security policies, principles, standards, and guidelines.

Agencies, in turn, are accountable for the effective and efficient development, acquisition, and use of information technology in their organizations. For example, the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 require agency heads, acting through agency CIOs, to

- better link their information technology planning and investment decisions to program missions and goals;
- develop and implement a sound information technology architecture;
- implement and enforce information technology management policies, procedures, standards, and guidelines;
- establish policies and procedures for ensuring that information technology systems provide reliable, consistent, and timely financial or program performance data; and
- implement and enforce applicable policies, procedures, standards, and guidelines on privacy, security, disclosure, and information sharing.

⁵This responsibility is in addition to OMB's role in assisting the President in reviewing agency budget submissions and compiling the President's budget, as discussed in 31 U.S.C. Chapter 11.

Another important organization in federal information resources and technology management—the CIO Council—was established by the President in July 1996. Specifically, Executive Order 13011 established the CIO Council as the principal interagency forum for improving agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council, chaired by OMB's Deputy Director for Management with a Vice Chair selected from among its members, is tasked with (1) developing recommendations for overall federal information technology management policy, procedures, and standards, (2) sharing experiences, ideas, and promising practices, (3) identifying opportunities, making recommendations for, and sponsoring cooperation in using information resources, (4) assessing and addressing workforce issues, (5) making recommendations and providing advice to appropriate executive agencies and organizations, and (6) seeking the views of various organizations. 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. With respect to Council resources, according to its charter, OMB and the General Services Administration are to provide support and assistance, which can be augmented by other Council members as necessary.

State and Foreign Government CIO Models Exist But Approaches Vary

CIOs or equivalent positions exist at the state level and in other countries, although no single preferred model has emerged. The specific roles, responsibilities, and authorities assigned to the CIO or CIO-type position vary, reflecting the needs and priorities of the particular government. This is consistent with research presented in our *Executive Guide: Maximizing the Success of Chief Information Officers—Learning from Leading Organizations*,⁶ which points out that there is no one right way to establish a CIO position and that leading organizations are careful to ensure that information management leadership positions are appropriately defined and implemented to meet their unique business needs.

Regardless of the differences in approach, the success of a CIO will typically rest on the application of certain fundamental principles. While our executive guide was specifically intended to help individual federal agencies maximize the success of their CIOs, several of the principles outlined in the guide also apply to the establishment of a governmentwide CIO. In particular, our research of leading organizations demonstrated that it is important for the organization to employ enterprisewide leaders who

⁶GAO/AIMD-00-83, Exposure Draft, March 2000.

embrace the critical role of information technology and reach agreement on the CIO's leadership role. Moreover, the CIO must possess sufficient stature within the organization to influence the planning process.

We have not evaluated the effectiveness of state and foreign government CIOs or equivalent positions; however, these positions appear to apply some of these same principles. With respect to the states, according to the National Association of State Information Resource Executives, the vast majority have senior executives with statewide authority for IT. State CIOs are usually in charge of developing statewide IT plans and approving statewide technical IT standards, budgets, personnel classifications, salaries, and resource acquisitions although the CIO's authority depends on the specific needs and priorities of the governors. Many state CIOs report directly to the state's governor with the trend moving in that direction. In some cases, the CIO is guided by an IT advisory board. As the president of the National Association of State Information Resource Executives noted in prior testimony before this Subcommittee, "IT is how business is delivered in government; therefore, the CIO must be a party to the highest level of business decisions . . . [and] needs to inspire the leaders to dedicate political capital to the IT agenda."⁷

National governments in other countries have also established a central information technology coordinating authority and, like the states, have used different implementation approaches in doing so. Preliminary results of a recent survey conducted by the International Council for Information Technology in Government Administration indicate that 8 of 11 countries surveyed have a governmentwide CIO, although the structure, roles, and responsibilities varied. Let me briefly describe the approaches employed by three foreign governments to illustrate this variety.

- Australia's Department of Communications, Information Technology and the Arts has responsibility for, among other things, (1) providing strategic advice and support to the government for moving Australia ahead in the information economy and (2) developing policies and procedures and helping to coordinate crosscutting efforts toward e-government.
- The United Kingdom's Office of the E-Envoy acts in a capacity analogous to a "national government" CIO in that it works to coordinate activities across government and with public, private, and international groups to

⁷Testimony of Otto Doll, President, National Association of State Information Resource Executives before the U.S. House of Representatives, Committee on Government Reform, Subcommittee on Government Management, Information and Technology, March 24, 2000.

(1) develop a legal, regulatory and fiscal environment that facilitates e-commerce, (2) help individuals and businesses take full advantage of the opportunities provided by information and communications technologies, (3) ensure that the government of the United Kingdom applies global best practices in its use of information and communications technologies, and (4) ensure that government and business decisions are informed by reliable and accurate e-commerce monitoring and analysis.

- Canada's Office of the CIO is contained within the Treasury Board Secretariat, a crosscutting organization whose mission is to manage the government's human, financial, information, and technology resources. The CIO is responsible for determining and implementing a strategy that will accomplish governmentwide IT goals. Moreover, the CIO is to (1) provide leadership, coordination and broad direction in the use of IT; (2) facilitate enterprisewide solutions to crosscutting IT issues; and (3) serve as technology strategist and expert adviser to Treasury Board Ministers and senior officials across government. The CIO also develops a Strategic Directions document that focuses on the management of critical IT, information management, and service delivery issues facing the government. This document is updated regularly and is used by departments and agencies as a guide.

While these countries' approaches differ in terms of specific CIO or CIO-type roles and responsibilities, in all cases the organization has responsibility for coordinating governmentwide implementation of e-government and providing leadership in the development of the government's IT strategy and standards.

Proposed Legislation Provides a Stronger Central Focus to the Government's Management of Information Technology

As you know, the Congress is currently considering legislation to establish a federal CIO. Specifically, two proposals before this Subcommittee—H.R. 4670, the Chief Information Officer of the United States Act of 2000, and H.R. 5024, the Federal Information Policy Act of 2000—share a common call for central IT leadership from a federal CIO, although they differ in how the roles, responsibilities, and authorities of the position would be established.

Several similarities exist in the two bills:

- Both elevate the visibility and focus of information resources and technology management by establishing a federal CIO who (1) is appointed by the President with the advice and consent of the Senate, (2) reports directly to the President, (3) is a Cabinet-level official, and (4) provides central leadership. The importance of such high level visibility

should not be underestimated. Our studies of leading public and private-sector organizations have found that successful CIOs commonly are full members of executive management teams.⁸

- Both leave intact OMB's role and responsibility to review and ultimately approve agencies' information technology funding requests for inclusion in the President's budget submitted to the Congress each year. However, both require the federal CIO to review and recommend to the President and the Director of OMB changes to the IT budget proposals submitted by agencies. As we have previously testified before your Subcommittee, an integrated approach to budgeting and feedback is absolutely critical for progress in government performance and management.⁹ Certainly, close coordination between the federal CIO and OMB would be necessary to coordinate the CIO's technical oversight and OMB's budget responsibilities.
- Finally, both bills establish the existing federal CIO Council in statute. Just as with the Chief Financial Officers' Council, there are important benefits associated with having a strong statutory base for the CIO Council. Legislative foundations transcend presidential administrations, fluctuating policy agendas, and the frequent turnover of senior appointees in the executive branch. Having congressional consensus and support for the Council helps ensure continuity of purpose over time and allows constructive dialogue between the two branches of government on rapidly changing management and information technology issues before the Council. Moreover, as prime users of performance and financial information, having the Council statutorily based can help provide the Congress with an effective oversight tool in gauging the progress and impact of the Council on advancing effective involvement of agency CIOs in governmentwide IT initiatives.

The two bills also set forth duties that are consistent with, and expand upon, the duties of the current CIO Council. For example, the Council would be responsible for coordinating the acquisition and provision of common infrastructure services to facilitate communication and data exchange among agencies and with state, local, and tribal governments.

⁸Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994) and GAO/AIMD-00-83, Exposure Draft, March 2000.

⁹Office of Management and Budget: Future Challenges to Management (GAO/T-GGD/AIMD-00-141, April 7, 2000).

While the bills have similarities, as a result of contrasting approaches, the two bills have major differences. In particular, H.R. 5024 vests in the federal CIO the information resources and technology management responsibilities currently assigned to OMB as well as oversight of related activities of the General Services Administration and promulgation of information system standards developed by the National Institute of Standards and Technology. On the other hand, H.R. 4670 generally does not change the responsibilities of these agencies; instead it calls on the federal CIO to advise agencies and the Director of OMB and to consult with nonfederal entities, such as state governments and the private sector.

Appendix I provides more detail on how information resources and technology management functions granted to the federal CIO compare among the two bills, and with OMB's current responsibilities.

Let me turn now to a few implementation issues associated with both of these bills. One such issue common to both is that effective implementation will require that appropriate presidential attention and support be given to the new federal CIO position and that adequate resources, including staffing and funding, be provided. As discussed below, each bill likewise has unique strengths and challenges.

- **H.R. 4670:** This bill creates an Office of Information Technology within the Executive Office of the President, headed by a federal CIO, with a limit of 12 staff. Among the duties assigned to the CIO are (1) providing leadership in innovative use of information technology, (2) identifying opportunities and coordinate major multi-agency information technology initiatives, and (3) consulting with leaders in information technology management in state governments, the private sector, and foreign governments. OMB's statutory responsibilities related to information resources and technology management would remain largely unchanged under this bill.

One strength of this bill is that it would allow a federal CIO to focus full-time attention on promoting key information technology policy and crosscutting issues within government and in partnership with other organizations without direct responsibility for implementation and oversight, which would remain the responsibility of OMB and the agencies. Moreover, the federal CIO could promote collaboration among agencies on crosscutting issues, adding Cabinet-level support to efforts now initiated and sponsored by the CIO Council. Further, the federal CIO could establish and/or buttress partnerships with state, local, and tribal governments, the private sector, or foreign entities. Such partnerships were key to the government's Year 2000 (Y2K) success and could be

essential to addressing other information technology issues, such as critical infrastructure protection, since private-sector systems control most of our nation's critical infrastructures (e.g., energy, telecommunications, financial services, transportation, and vital human services).

A major challenge associated with H.R. 4670's approach, on the other hand, is that federal information technology leadership would be shared. While the CIO would be the President's principal adviser on these issues, OMB would retain critical statutory responsibilities in this area. For example, both the federal CIO and OMB would have a role in overseeing the government's IT and interagency initiatives. Certainly, it would be crucial for the OMB Director and the federal CIO to mutually support each other and work effectively together to ensure that their respective roles and responsibilities are clearly communicated. Without a mutually constructive working relationship with OMB, the federal CIO's ability to achieve the potential improvements in IT management and cross-agency collaboration would be impaired.

- **H.R. 5024:** This bill establishes an Office of Information Policy within the Executive Office of the President and headed by a federal CIO. The bill would substantially change the government's existing statutory information resources and technology management framework because it shifts much of OMB's responsibilities in these areas to the federal CIO. For example, it calls for the federal CIO to develop and oversee the implementation of policies, principles, standards, and guidance with respect to (1) information technology, (2) privacy and security, and (3) information dissemination.

A strength of this approach would be the single, central focus for information resources and technology management in the federal government. A primary concern we have with OMB's current structure as it relates to information resources and technology management is that, in addition to their responsibilities in these areas, both the Deputy Director for Management and the Administrator of the Office of Information and Regulatory Affairs (OIRA) have other significant duties, which necessarily restrict the amount of attention that they can give to information resources and technology management issues.¹⁰ For example, much of OIRA is staffed to act on 3,000 to 5,000 information collection requests from agencies per year, review about 500 proposed and final rules each

¹⁰While OMB's Director is responsible for these functions, they have generally been delegated to the Office of Information and Regulatory Affairs, which reports to the Deputy Director for Management.

year, and to calculate the costs and benefits of all federal regulations. A federal CIO, like agency CIOs, should be primarily concerned with information resources and technology management. This bill would clearly address this concern.

Another important strength of H.R. 5024 is that the federal CIO would be the sole central focus for information resources and technology management and could be used to resolve potential conflicts stemming from conflicting perspectives or goals within the executive branch agencies.

In contrast, a major challenge associated with implementing H.R. 5024 is that by removing much of the responsibility for information resources and technology management from OMB, the federal CIO could lose the leverage associated with OMB's budget-review role. A strong linkage with the budget formulation process is often a key factor in gaining serious attention for management initiatives throughout government, and reinforces the priorities of federal agencies' management goals.

Central and Effective Federal Information Resources and Technology Management Leadership Is Needed

Regardless of approach, we agree that strong and effective central information resources and technology management leadership is needed in the federal government. A central focal point such as a federal CIO can play the essential role of ensuring that attention in these areas is sustained. Increasingly, the challenges the government faces are multidimensional problems that cut across numerous programs, agencies, and governmental tools. Although the respective departments and agencies should have the primary responsibility and accountability to address their own issues—and both bills maintain these agency roles—central leadership has the responsibility to keep everybody focused on the big picture by identifying the agenda of governmentwide issues needing attention and ensuring that related efforts are complementary rather than duplicative. Another task facing central leadership is serving as a catalyst and strategist to prompt agencies and other critical players to come to the table and take ownership for addressing the agenda of governmentwide information resources and technology management issues.

In the legislative deliberations on the Clinger-Cohen Act, we supported strengthened central management through the creation of a formal CIO

position for the federal government.¹¹ A CIO for the federal government could provide a strong, central point of coordination for the full range of governmentwide information resources management and technology issues, including (1) reengineering and/or consolidating interagency or governmentwide process and technology infrastructure; (2) managing shared assets; and (3) evaluating attention, progress evaluations, and assistance provided to high-risk, complex information systems modernization efforts.

In particular, a federal CIO could provide sponsorship, direction, and sustained focus on the major challenges the government is facing in areas such as critical infrastructure protection and security, e-government, and large-scale IT investments. For example, to be successful, e-government initiatives designed to improve citizen access to government must overcome some of the basic challenges that have plagued information systems for decades – lack of executive level sponsorship, involvement, and controls; inadequate attention to business and technical architectures; adherence to standards; and security. In the case of e-government, a CIO could (1) help set priorities for the federal government; (2) ensure that agencies consider interagency web site possibilities, including how best to implement portals or central web access points that provide citizens access to similar government services; and (3) help establish funding priorities, especially for crosscutting e-government initiatives.

The government's success in combating the Year 2000 problem demonstrated the benefit of strong central leadership. As our Year 2000 lessons learned report being released today makes clear, the leadership of the Chair of the President's Council on Year 2000 Conversion was invaluable in combating the Year 2000 problem.¹² Under the Chair's leadership, the government's actions went beyond the boundaries of individual programs or agencies and involved governmentwide oversight, interagency cooperation, and cooperation with partners, such as state and local governments, the private sector, and foreign governments.

It is important to maintain this same momentum of executive-level attention to information management and technology decisions within the

¹¹*Improving Government: Actions Needed to Sustain and Enhance Management Reforms* (GAO/T-OCG-94-1, January 27, 1994), *Government Reform: Using Reengineering and Technology to Improve Government Performance* (GAO/T-OCG-95-2, February 2, 1995), and *Government Reform: Legislation Would Strengthen Federal Management of Information and Technology* (GAO/T-AIMD-95-205, July 25, 1995).

¹²*Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenge* (GAO/AIMD-00-290, September 12, 2000).

federal government. The information issues confronting the government in the new Internet-based technology environment rapidly evolve and carry significant impact for future directions. A federal CIO could maintain and build upon Y2K actions in leading the government's future IT endeavors. Accordingly, our Y2K lessons learned report calls for the Congress to consider establishing a formal chief information officer position for the federal government to provide central leadership and support.

Consensus has not been reached within the federal community on the need for a federal CIO. Department and agency responses to questions developed by the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs regarding opinions about the need for a federal CIO found mixed reactions. In addition, at our March 2000 Y2K Lessons Learned Summit, which included a broad range of public and private-sector IT managers and policymakers, some participants did not agree or were uncertain about whether a federal CIO was needed. Further, in response to a question before this Subcommittee on the need for a federal IT leader accountable to the President, the Director of OMB stated that OMB's Deputy Director for Management, working with the head of the Office of Information and Regulatory Affairs, can be expected to take a federal information technology leadership role. The Director further stated that he believed that "the right answer is to figure out how to continue to use the authority and the leadership responsibilities at the Office of Management and Budget to play a lead role in this [IT] area."

In conclusion, Mr. Chairman, the two bills offered by members of this Subcommittee both deal with the need for central leadership, while addressing the sharing of responsibilities with OMB in different ways. Both bills offer different approaches to problems that have been identified and should be dealt with in order to increase the government's ability to use the information resources at its disposal effectively, securely, and with the best service to the American people. Regardless of approach, a central focal point such as a federal CIO can play the essential role of ensuring that attention to information technology issues is sustained.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the Subcommittee may have at this time.

Contacts and Acknowledgments

For information about this testimony, please contact me at (202) 512-6240 or by e-mail at mcclured.aimd@gao.gov. Individuals making key contributions to this testimony include John Christian, Lester Diamond,

Tamra Goldstein, Linda Lambert, Thomas Noone, David Plocher, and
Tomas Ramirez.

Appendix I

Comparison of OMB's Current Functions and Those Assigned to the Federal CIO by H.R. 4670 and H.R. 5024

Function	OMB's Current Functions ^a	CIO Responsibility	
		H.R. 4670	H.R. 5024
Budget	<p>Develop, as part of the budget process, a mechanism for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems.</p> <p>Implement periodic budgetary reviews of agency information resources management activities to ascertain efficiency and effectiveness of IT in improving agency mission performance.</p> <p>Take actions through the budgetary and appropriations management process to enforce agency accountability for information resources management and IT investments, including the reduction of funds.</p>	<p>Review and recommend to the President and the Director of OMB changes to budget and legislative proposals of agencies.</p>	<p>Review and recommend to the President and the Director of OMB changes to budget and legislative proposals of agencies.</p> <p>Advise and assist the Director of OMB in developing, as part of the budget process, a mechanism for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems.</p> <p>Implement periodic budgetary reviews of agency information resources management activities to ascertain efficiency and effectiveness of IT in improving agency mission performance.</p> <p>Request that the Director of OMB take action, including involving the budgetary or appropriations management process, to enforce agency accountability for information resources management and IT investments, including the reduction of funds.</p>
CIO Council	The Deputy Director for Management serves as the Chairperson of the CIO Council, which was created by Executive Order.	Serves as the Chairperson of the CIO Council, established by the bill in statute.	Serves as the Chairperson of the CIO Council, established by the bill in statute.
Electronic records	<p>In consultation with the Administrator of the National Telecommunications and Information Administration, develop and implement procedures for the use and acceptance of electronic signatures by agencies by April 21, 2000.</p> <p>Ensure that, no later than October 21, 2003, agencies provide for the option of the electronic maintenance, submission or disclosure of information and for the use and acceptance of electronic signatures, where</p>	Advise the Director of OMB on electronic records. ^b	<p>In consultation with the Director of OMB and the Administrator of the National Telecommunications and Information Administration, develop and implement procedures for the use and acceptance of electronic signatures by agencies by October 1, 2000.</p> <p>Ensure that, no later than October 1, 2003, agencies provide for the option of the electronic maintenance, submission or disclosure of information and for the use and acceptance of electronic signatures, where</p>

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Function	OMB's Current Functions ^a	CIO Responsibility	
		H.R. 4670	H.R. 5024
Electronic records (cont'd)	<p>practicable.</p> <p>Develop and implement procedures to permit private employers to store and file electronically with agencies forms containing information pertaining to the employees of such employers.</p> <p>In consultation with the Administrator of the National Telecommunications and Information Administration study and periodically report on the use of electronic signatures.</p>		<p>practicable.</p> <p>In consultation with the Director of OMB, develop and implement procedures to permit private employers to store and file electronically with agencies forms containing information pertaining to the employees of such employers.</p> <p>In consultation with the Director of OMB and the Administrator of the National Telecommunications and Information Administration study and periodically report on the use of electronic signatures.</p> <p>Assisted by the CIO Council and others, monitor the implementation of the requirements of the Government Paperwork Elimination Act, the Electronic Signatures in Global and National Commerce Act and related laws.</p>
Information dissemination	<p>Provide direction and oversee activities of agencies with respect to the dissemination of and public access to information.</p> <p>Foster greater sharing, dissemination, and access to public information.</p> <p>Develop and oversee the implementation of policies, principles, standards, and guidance with respect to information dissemination.</p> <p>Cause to be established and oversee an electronic Government Information Locator Service (GILS).</p>	<p>Advise the Director of OMB on information dissemination.⁷</p>	<p>Provide direction and oversee activities of agencies with respect to the dissemination of and public access to information.</p> <p>Foster greater sharing, dissemination, and access to public information.</p> <p>Develop and oversee the implementation of policies, principles, standards, and guidance with respect to information dissemination.</p> <p>Cause to be established and oversee an electronic GILS.</p>
Information resources management policy	<p>Develop, coordinate, and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines.</p> <p>Oversee the development and</p>	<p>Advise the Director of OMB on information resources management policy.⁸</p>	<p>Develop, coordinate, and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines.</p> <p>Oversee the development and</p>

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Function	OMB's Current Functions ^a	CIO Responsibility	
		H.R. 4670	H.R. 5024
Information resources management policy (cont'd)	<p>implementation of best practices in information resources management.</p> <p>Oversee agency integration of program and management functions with information resources management functions.</p> <p>In consultation with the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Archivist of the United States, and the Director of the Office of Personnel Management, develop and maintain a governmentwide strategic plan for information resources management.</p> <p>Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices.</p> <p>Monitor information resources management training for agency personnel.</p> <p>Keep the Congress informed on the use of information resources management best practices to improve agency program performance.</p> <p>Periodically review agency information resources management activities.</p> <p>Report annually to the Congress on information resources management.</p>		<p>implementation of best practices in information resources management.</p> <p>Oversee agency integration of program and management functions with information resources management functions.</p> <p>In consultation with the Director of OMB, the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Archivist of the United States, the Director of the Office of Personnel Management, and the CIO Council, develop and maintain a governmentwide strategic plan for information resources management.</p> <p>Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices.</p> <p>Monitor information resources management training for agency personnel.</p> <p>Keep the Congress informed on the use of information resources management best practices to improve agency program performance.</p> <p>Periodically review agency information resources management activities.</p> <p>Report annually to the Congress on information resources management.</p>
Information technology management	In consultation with the National Institute of Standards and Technology and the General Services Administration, develop and oversee the implementation of	Serve as the principal adviser to the President on matters relating to the development, application, and management of IT by the federal government.	Serve as the principal adviser to the President on matters related to the efficient and effective development, use, and management of IT and other

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Function	OMB's Current Functions ^a	CIO Responsibility	
		H.R. 4670	H.R. 5024
Information technology management (cont'd)	policies, principles, standards, and guidelines for IT functions and activities.	Advise the President on opportunities to use IT to improve the efficiency and effectiveness of programs and operations of the federal government.	information resources by the federal government.
	Ensure that agencies integrate information resources plans, program plans, and budgets for acquisition and use of technology.	Advise the Director of OMB on IT management. ^b	Develop and oversee the implementation of policies, principles, standards, and guidelines for IT functions and activities, in consultation with the Secretary of Commerce and the CIO Council.
	Provide direction and oversee activities of agencies with respect to the acquisition and use of IT.	Report annually to the President and the Congress on IT management.	Promulgate, in consultation with the Secretary of Commerce, standards and guidelines for federal information systems.
	Promote the use of IT by the federal government to improve the productivity, efficiency, and effectiveness of federal programs.	Promote agency investments in IT that enhance service delivery to the public, improve cost-effective government operations, and serve other objectives critical to the President.	Review the federal information system standards setting process, in consultation with the Secretary of Commerce, and report to the President.
	Oversee the effectiveness of, and compliance with, directives issued under section 110 of the Federal Property and Administrative Services Act (which established the Information Technology Fund).	Direct the use of the Information Technology Fund by the Administrator of General Services.	Provide advice and assistance to the Administrator of the Office of Federal Procurement Policy regarding IT acquisition.
	Coordinate OIRA policies regarding IT acquisition with the Office of Federal Procurement Policy.	Consult with leaders in state governments, the private sector, and foreign governments.	Ensure that agencies integrate information resources plans, program plans, and budgets for acquisition and use of technology.
	Oversee the development and implementation of computer system standards and guidance issued by the Secretary of Commerce through the National Institute of Standards and Technology.		Provide direction and oversee activities of agencies with respect to the acquisition and use of IT.
	Designate agencies, as appropriate, to be executive agents for governmentwide acquisitions of IT.		Promote the use of IT by the federal government to improve the productivity, efficiency, and effectiveness of federal programs.
	Compare agency performance in using IT.		Establish minimum criteria within 1 year of enactment to be used for independent evaluations of IT programs and management processes.
	Encourage use of performance-based management in complying with IT management requirements.		Direct and oversee all actions by the Administrator of General

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Function	OMB's Current Functions*	CIO Responsibility	
		H.R. 4670	H.R. 5024
Information technology management (cont'd)	Evaluate agency practices with respect to the performance of investments made in IT.		Services with regard to the provision of any information resources-related services for or on behalf of agencies, including the acquisition or management of telecommunications or other IT or services.
	Direct agencies to develop capital planning processes for managing major IT investments.		Direct the use of the Information Technology Fund by the Administrator of General Services.
	Direct agencies to analyze private sector alternatives before making an investment in a new information system.		Oversee the effectiveness of, and compliance with, directives issued under section 110 of the Federal Property and Administrative Services Act (which established the Information Technology Fund).
	Direct agencies to undertake an agency mission reengineering analysis before making significant investments in IT to support these missions.		Oversee the development and implementation of computer system standards and guidance issued by the Secretary of Commerce through the National Institute of Standards and Technology.
			Designate agencies, as appropriate, to be executive agents for governmentwide acquisitions of IT.
			Compare agency performance in using IT.
			Encourage use of performance-based management in complying with IT management requirements.
			Evaluate agency practices with respect to the performance of investments made in IT.
			Direct agencies to develop capital planning processes for managing major IT investments.
			Direct agencies to analyze private sector alternatives before making an investment in a new information system.

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Function	OMB's Current Functions*	H.R. 4670	CIO Responsibility
			H.R. 5024
Information technology management (cont'd)			Direct agencies to undertake an agency mission reengineering analysis before making significant investments in IT to support these missions.
Innovation	<p>Conduct pilot projects with selected agencies and nonfederal entities to test alternative policies and practices.</p> <p>Assess experiences of agencies, state and local governments, international organizations, and the private sector in managing IT.</p>	<p>Provide leadership in the innovative use of technology by agencies through support of experimentation, testing, and adoption of innovative concepts and technologies, particularly with regard to multi-agency initiatives.</p>	<p>Conduct pilot projects with selected agencies and nonfederal entities to test alternative policies and practices.</p> <p>Provide leadership in the innovative use of technology by agencies through support of experimentation, testing, and adoption of innovative concepts and technologies, particularly with regard to multi-agency initiatives.</p> <p>Assess experiences of agencies, state and local governments, international organizations, and the private sector in managing IT.</p>
Interagency cooperation	<p>Ensure the efficiency and effectiveness of interagency IT initiatives.</p> <p>Issue guidance to agencies regarding interagency and governmentwide IT investments to improve the accomplishment of common missions and for the multiagency procurement of commercial IT items.</p>	<p>Identify opportunities and coordinate major multiagency IT initiatives.</p>	<p>Ensure the efficiency and effectiveness of interagency IT initiatives.</p> <p>Issue guidance to agencies regarding interagency and governmentwide IT investments to improve the accomplishment of common missions and for the multiagency procurement of commercial IT items.</p>
National security systems	<p>Apply capital planning, investment control, and performance management requirements to national security systems to the extent practicable.</p>	<p>Consult with the heads of agencies that operate national security systems.</p>	<p>Consult with the heads of agencies that operate national security systems.</p> <p>Apply capital planning, investment control, and performance management requirements to national security systems to the extent practicable.</p>

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Paperwork reduction	Review agency collections of information to reduce paperwork burdens on the public.	Advise the Director of OMB on paperwork reduction. ^b	Provide advice and assistance to agencies and to the Director of OMB to promote efficient collection of information and the reduction of paperwork burdens on the public.
Privacy and security	<p>Provide direction and oversee activities of agencies with respect to privacy, confidentiality, security, disclosure, and sharing of information.</p> <p>Develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of agency information.</p> <p>Oversee and coordinate compliance with the Privacy Act, the Freedom of Information Act, the Computer Security Act, and related information management laws.</p> <p>Require federal agencies, consistent with the Computer Security Act, to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of agency information.</p> <p>Review agency computer security plans required by the Computer Security Act.</p> <p>Oversee agency compliance with the Privacy Act.</p>	Advise the Director of OMB on privacy, confidentiality, security, disclosure, and sharing of information. ^b	<p>Provide direction and oversee activities of agencies with respect to privacy, confidentiality, security, security, disclosure, and sharing of information.</p> <p>Develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of agency information. Oversee and coordinate compliance with the Privacy Act, the Freedom of Information Act, the Computer Security Act, and related information management laws.</p> <p>Require federal agencies, consistent with the Computer Security Act, to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of agency information collected or maintained.</p> <p>Establish governmentwide policies for promoting risk-based management of information security as an integral component of each agency's business operations.</p> <p>Direct agencies to use best security practices, develop an agencywide security plan, and apply information security requirements throughout the information system life cycle.</p> <p>Review agency computer security plans required by the Computer Security Act.</p>

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Privacy and security (cont'd)	Records management	Provide direction and oversee activities of agencies with respect to records management activities.	Advise the Director of OMB on records management. ^b	Oversee agency compliance with the Privacy Act.
				Provide direction and oversee activities of agencies with respect to records management activities.
		Provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination of records management with information resources management requirements.		Provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination of records management with information resources management requirements.
				Review agency compliance with requirements and regulations. Oversee the application of records management policies, principles, standards, and guidelines in the planning and design of information systems.
Statistical policy and coordination		Provide direction and oversee activities of agencies with respect to statistical activities.	Advise the Director of OMB on statistical policy and coordination. ^b	Provide direction and oversee activities of agencies with respect to statistical activities.
				Coordinate the activities of the federal statistical system.
		Ensure that agency budget proposals are consistent with systemwide priorities for maintaining and improving the quality of federal statistics.		Consult with the Director of OMB to ensure that agency budget proposals are consistent with systemwide priorities for maintaining and improving the quality of federal statistics.
				Develop and oversee governmentwide statistical policies, principles, standards, and guidelines.
		Evaluate statistical program performance and agency compliance with governmentwide statistical policies, principles, standards, and guidelines.		Evaluate statistical program performance and agency compliance with governmentwide statistical policies, principles, standards, and guidelines.
				Promote the sharing of information collected for statistical purposes.
		Promote the sharing of information collected for statistical purposes.		Promote the sharing of information collected for statistical purposes.
				Coordinate the U.S. participation in international statistical activities.

Appendix I
Comparison of OMB's Current Functions
and Those Assigned to the Federal CIO by
H.R. 4670 and H.R. 5024

Statistical policy and coordination (cont'd)	Establish an Interagency Council on Statistical Policy, headed by an appointed chief statistician.	Establish an Interagency Council on Statistical Policy, headed by an appointed chief statistician.
	Provide opportunities for training in statistical policy.	Provide opportunities for training in statistical policy.

*While OMB's Director is responsible for these functions, they have generally been delegated to the Office of Information and Regulatory Affairs, which reports to the Deputy Director for Management. These functions are outlined in the Privacy Act of 1974, the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Government Paperwork Elimination Act of 1998.

*H.R. 4670 specifically authorizes the CIO to advise the Director of OMB to "ensure effective implementation of the functions and responsibilities under assigned under chapter 35 of title 44, United States Code." These functions include electronic records (through the Government Paperwork Elimination Act of 1998), information dissemination, information resources management policy, information technology management, paperwork reduction, privacy and security, records management, and statistical policy and coordination.

(512023)

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)

GAO

United States General Accounting Office

Report to the Chairman, Subcommittee
on Government Management,
Information and Technology, Committee
on Government Reform, House of
Representatives

September 2000

YEAR 2000 COMPUTING CHALLENGE

Lessons Learned Can
Be Applied to Other
Management
Challenges

**G A O**

Accountability • Integrity • Reliability

GAO/AIMD-00-290

Contents

Letter	3
<hr/>	
Appendixes	
Appendix I: Timeline of Major Y2K Events	44
Appendix II: Participants in GAO's Y2K Lessons Learned Summit	52
Appendix III: GAO Reports and Testimony Statements Addressing the Year 2000 Computing Challenge	55
Appendix IV: Comments From the Office of Management and Budget	69

Abbreviations

CIO	chief information officer
DOD	Department of Defense
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
HCFA	Health Care Financing Administration
IT	information technology
IV&V	independent validation and verification
OMB	Office of Management and Budget
PDD	Presidential Decision Directive 63
Y2K	Year 2000



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

Accounting and Information
Management Division

B-286056

September 12, 2000

The Honorable Stephen Horn
Chairman, Subcommittee on Government
Management, Information and Technology
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Since the early 1990s, an explosion of computer interconnectivity, most notably the growth of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity poses great risks to our computer systems and the critical operations and infrastructures they support. The Year 2000 (Y2K) challenge was a major test of the nation's ability to protect these critical systems and operations.

Because of the urgent nature and potential impact of the Y2K problem on critical government operations, in February 1997 we designated it a high-risk area for the federal government.¹ Our purpose was to stimulate greater attention to assessing the government's exposure to Y2K risks and to strengthen planning for achieving Y2K compliance for mission-critical systems.

To help agencies mitigate their Y2K risks, we produced a series of guides and reports. Our guides provided systematic approaches to enterprise readiness, business continuity and contingency planning, testing, and day one planning.² Federal agencies and other organizations used these guides widely to help organize and manage their Year 2000 programs. In addition,

¹High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

²Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998), Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998) and Year 2000 Day One Planning and Operations Guide (GAO/AIMD-10.1.22, October 1999).

B-286056

we issued over 160 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 readiness of both the government as a whole and a wide range of individual federal agencies. Our recommendations were almost universally embraced. (A list of these reports and testimony statements can be found in appendix III.)

By successfully meeting the Y2K challenge, the government passed a major test of its ability to protect the nation's computer-supported critical infrastructure. However, major management challenges remain in areas such as computer security and critical infrastructure protection. At your request, this report (1) identifies lessons the federal government has learned from Y2K applicable to improving federal information technology (IT) management, (2) identifies lessons that individual agencies can apply to management of future IT initiatives, and (3) discusses how the momentum generated by the government's Y2K efforts can be sustained.

Results in Brief

The Y2K challenge was met through the collaborative efforts of the Congress, the administration, federal agencies, state and local governments, and the private sector. Had any of these sectors failed to take the Y2K problem seriously, neglected to remediate computer systems, or failed to work together with partners on common issues, such as contingency planning, critical services could have been disrupted.

Although the Y2K crisis was finite, it led to the development of initiatives, processes, methodologies, and experiences that can assist in resolving ongoing management challenges. First, Y2K demonstrated the value of sustained and effective bipartisan oversight by both the Senate and the House of Representatives; they highlighted the issue and provided needed resources. Second, leadership, commitment, and coordination by the federal government, which included periodic reporting and oversight of agency efforts, were major reasons for the government's Y2K success. Third, the President's Council on Year 2000 Conversion and individual agencies formed working partnerships with other agencies, states, other countries, and the private sector. Fourth, communication within agencies, with partners, and with the public was vital to coordinating efforts and ensuring an appropriate public response. Finally, the federal government implemented initiatives that helped ensure that necessary staff and financial resources would be available to agencies.

Individual agencies also gleaned lessons from their Y2K efforts that can be carried forward. Specific management practices that contributed to Y2K

B-286056

success included top-level management attention, risk analysis, project management, development of complete information systems inventories and strengthened configuration management, independent reviews by internal auditors and independent contractors, improved testing methods and procedures, and business continuity and contingency planning. By continuing and strengthening these practices in the future, federal agencies are more likely to improve their overall IT management record, particularly in the areas of critical infrastructure protection and security, the effective use of technology, and large-scale IT investments.

It is critical that the momentum generated by the government's Y2K efforts not be lost. The priority both the legislative and executive branches gave to the Y2K challenge and the persistence they both demonstrated were crucial to its successful outcome. Specifically, strong and focused leadership providing undivided attention and direction was a pivotal factor leading to Y2K success. Applying this leadership lesson to other ongoing major management issues—such as computer security and critical infrastructure protection—will also be essential to adequately confronting these and other challenges.

Background

The federal government was highly vulnerable to Year 2000-related computer problems because of its widespread dependence on computer systems to process financial transactions, deliver public services, and carry out its operations. Further, the many interdependencies among governments and within key economic sectors could have caused a single failure to have additional adverse repercussions. The public faced the risk that critical services provided by the government and the private sector could be disrupted by the change of century rollover. Financial transactions could have been delayed, flights grounded, power lost, and national defense affected.

B-286056

Growing Concern Led to Increased Federal Y2K Response

The federal government was slow initially in addressing Y2K, but as the date grew closer, the government's response improved. Specifically, at the urging of congressional leaders and others, the Office of Management and Budget (OMB) and federal agencies dramatically increased the amount of attention and oversight given to the Year 2000 issue.³ By 1999, according to OMB's Director, the administration had designated resolving the Y2K problem as its foremost management objective. Appendix I provides a timeline of significant Y2K events and illustrates (1) the increased attention as the century date change grew closer and (2) many of the organizations that played a key role in coordinating the government's response to the Y2K issue.

One organization in particular—the President's Council on Year 2000 Conversion—played an essential role in the government's response. The Council was established by the President in February 1998, and its Chair was tasked with (1) overseeing the activities of agencies, (2) acting as chief spokesperson in national and international forums, (3) providing policy coordination of executive branch activities with state, local, and tribal governments, and (4) promoting appropriate federal roles with respect to private-sector activities. The President also set the goal that no system critical to the federal government's mission would experience disruption because of Y2K and charged agency heads with ensuring that this issue received the highest priority.

Agencies' progress in achieving Y2K compliance demonstrated the government's tremendous improvement in addressing the Y2K problem. For example, in May 1997 OMB reported that 21 percent of the 24 major federal departments and agencies' mission-critical systems were compliant, but by December 1999, it reported that 99.9 percent of these systems were compliant. As a result of this progress, during the century change and leap day rollover period, most Year 2000-related errors reported by the federal government were minor and did not have an effect on operations or the delivery of services.⁴ Even those that were significant (that resulted in degraded service or, if not corrected, would have so resulted) were mitigated by quick action to fix the problems or by

³Year 2000 Computing Challenge: Noteworthy Improvements in Readiness But Vulnerabilities Remain (GAO/T-AIMD-00-37, November 4, 1999).

⁴Year 2000 Computing Challenge: Leadership and Partnerships Result in Limited Rollover Disruptions (GAO/T-AIMD-00-70, January 27, 2000).

B-286056

implementing contingency plans. Examples of Y2K problems that occurred during the century change rollover follow.

- On January 1, 2000, the Deputy Secretary of Defense reported that one of its satellite-based intelligence systems experienced a Y2K failure shortly after the rollover of Greenwich Mean Time; the Department of Defense (DOD) was not able to process information from that system. According to the Deputy Secretary, the problem was with the ground processing station, not the satellite itself. The Deputy Secretary also stated that DOD adopted backup procedures, which resulted in its operating at less than its full peacetime level of activity but allowed it to continue to meet its high-priority needs. DOD reported that the satellite ground processing system was returned to full operational status on January 3, 2000.
- Medicare provider claims were returned because claims were submitted dated 1900 or 2099. Some Medicare data centers reported that they received claims from providers with these erroneous dates after the rollover. For example, as of mid-February, the Health Care Financing Administration (HCFA) reported that 45 contractors had received at least 50,475 claims from 872 submitters with service dates of 1900 or 2099. According to HCFA's Deputy Director of Information Services, most of these claims were traced to providers that had not upgraded their systems.
- The Federal Aviation Administration's (FAA) air traffic control system reported experiencing Year 2000-related systems problems. However, according to FAA, no problem affected safety, service, or capacity, and some merely involved inaccurate date displays. In all cases, FAA reported that it was able to quickly fix the system or implement contingency plans that allowed operations to continue. Two key systems that did experience problems were the Low Level Wind Shear Alert System and a contractor-maintained Kavouras Graphic Weather Display System. In the case of the Low Level Wind Shear Alert System, the system displayed an error at eight sites following the rollover from 1999 to 2000 Greenwich Mean Time and failed to operate. All systems were back to normal in about 2 hours, but this problem could have affected aviation operations if weather conditions had been severe. In the case of the Kavouras Graphic Weather Display System, 10 minutes after the Greenwich Mean Time rollover, the system began sending data showing the year as 2010. This resulted in the system's rejecting weather data from the National Weather Service and failing to properly update data going to 13 Automated Flight Service Stations.

B-286056

Federal agencies also worked with state partners to prepare for the date change. For example, the Departments of Agriculture, Health and Human Services, and Labor took action to help states successfully move the 10 state-administered federal programs into the year 2000. The success of these efforts is demonstrated by the relatively minor Year 2000-related errors reported in these programs during the century change and leap day rollover period, which included the following.

- Oregon had Year 2000-related errors in systems used for the Food Stamps, Child Support Enforcement, and Temporary Assistance for Needy Families programs during the century rollover. Regarding food stamps, the state's system for processing daily updates failed, creating a backlog of batch records. This problem was corrected by the installation of a new system on the next business day, and no impact on business operations was reported. The state system that tracks data in numerous programs, including Child Support Enforcement and Temporary Assistance for Needy Families, had a Year 2000-related problem that was fixed by January 7, 2000. This problem resulted in a 1-day delay in payments to clients.
- Louisiana reported that its Medicaid Eligibility Verification System suffered about a 10-hour service interruption on February 29 when it did not recognize the date as valid. The Louisiana report indicated that alternate eligibility verification systems were available and that no recipients should have been denied services.

The Federal Government Continues to Face Major Management Challenges

American citizens are increasingly demanding improved government services and better stewardship of public resources. Responding to these demands will require government decisionmakers to adopt new ways of thinking, consider different ways of achieving goals, and use new types of information to guide decisions. In 1999 we issued a series of reports—our Performance and Accountability Series—that describes management challenges confronting individual agencies and the government as a whole.⁵ We noted that the Congress has put in place a statutory framework for performance-based management but that many agencies continue to struggle with its basic tenets. In particular, the government faced challenges

⁵Major Management Challenges and Program Risks: An Executive Summary (GAO/OCG-99-ES, February 1999) provides an overview of this series.

B-286066

- adopting a results orientation;
- effectively using IT to help achieve program results;
- establishing financial management capabilities that effectively support informed decision-making and accountability; and
- building, maintaining, and marshaling human capital needed to achieve results.

The Performance and Accountability Series complemented our existing High-Risk Series. Since 1990, we have periodically reported on government operations that we have identified as high risk because of their greater vulnerability to waste, fraud, abuse, or mismanagement. For example, we have designated information security and four agency IT modernization efforts (the Internal Revenue Service's tax systems modernization, FAA's Air Traffic Control Modernization, and modernization efforts at DOD and the National Weather Service) as high risk.⁵

Regarding improving federal government operations, legislation such as the Chief Financial Officers Act of 1990, the Federal Acquisition Streamlining Act of 1994, the Paperwork Reduction Act of 1995, the Federal Financial Management Improvement Act of 1996, and the Clinger-Cohen Act of 1996 set forth requirements for more effective use of IT. For example, the Clinger-Cohen Act requires agencies to focus more on the results achieved through IT investments.

⁵High-Risk Series: An Overview (GAO/HR-95-1, February 1995), GAO/HR-97-9, February 1997, and High Risk Series: An Update (GAO/HR-99-1, January 1999).

B-286056

With respect to improving information security, Presidential Decision Directive 63 (PDD 63), issued in May 1998, sets as an objective that within 5 years of its signing, the United States will achieve the ability to protect our nation's critical infrastructures. It requires that the executive branch assess the cyber vulnerabilities of the nation's critical infrastructures—information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health as well as those authorities responsible for continuity of federal, state, and local governments. The directive places special emphasis on protecting the government's own critical assets from cyber attack and the need to remedy deficiencies in order to become a model of information security. Various activities have been undertaken in response to PDD 63, including development and review of individual agency critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links. In January 2000, the White House released its National Plan for Information Systems Protection as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks.⁷

Objectives, Scope, and Methodology

The objectives of this review were to identify (1) lessons the federal government has learned from Y2K applicable to improving future federal IT management governmentwide, (2) lessons that individual agencies can apply to management of future IT initiatives, and (3) how the momentum generated by the government's Y2K efforts can be sustained.

To identify lessons learned from the Y2K experience, we

- conducted a Y2K Lessons Learned Summit at GAO involving 22 attendees from the legislative and executive branches of government and the private sector (see appendix II for a list of participants) to (1) examine what lessons the government has learned from the Y2K challenge and how momentum can be maintained to sustain improved IT management and address critical infrastructure issues and

⁷*Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, The White House, January 7, 2000. See *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/T-AIMD-00-72, February 1, 2000) for our comments on this plan.

B-286056

- (2) determine what mechanisms are needed to ensure that the critical factors behind the government's Y2K success remain in place;
- contacted the 24 major federal departments and agencies, 9 of which provided us with formal lessons learned that they had developed; and
 - reviewed documents developed by other organizations, such as the President's Council on Year 2000 Conversion, the U.S. Senate Special Committee on the Year 2000 Technology Problem, and the United Nations' International Y2K Cooperation Center.⁵

We performed our review between March and mid-August 2000 in Washington D.C., in accordance with generally accepted government auditing standards, except that we did not assess the validity of agency lessons learned documents. OMB provided us with comments on a draft of this report. These comments are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix IV.

Leadership and Partnerships Were Key to the Nation's Successful Y2K Oversight and Coordination

The value of federal government leadership, oversight, and partnerships to the nation's successful Y2K outcome was repeatedly cited by agencies and Y2K Lessons Learned Summit participants. Government actions went beyond the boundaries of individual programs or agencies and involved governmentwide oversight, interagency cooperation, and cooperation among federal, state, and local governments; private sector entities; and foreign countries. These broad efforts can be grouped into five categories:

- congressional oversight,
- central leadership and coordination,
- partnerships,
- communications, and
- human capital and budget initiatives.

⁵The International Y2K Cooperation Center was created by the United Nations to promote strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on global society and the economy.

The Congress Played a Key Oversight Role

Sustained bipartisan and bicameral congressional leadership played a key role in addressing the Year 2000 challenge by holding agencies responsible for demonstrating progress and by heightening public awareness of the problem. According to the final report of the Senate Special Committee on the Year 2000 Technology Problem,⁹ its bipartisan, cooperative approach was a vital aspect of its role. Moreover, at the Y2K Lessons Learned Summit, the co-chairs of the House Year 2000 Task Force emphasized the effectiveness of the bipartisan manner in which the Congress addressed the Y2K problem.

Committees and subcommittees in both the Senate and the House of Representatives held many hearings on the Year 2000 issue. According to the Congressional Research Service, congressional committees and subcommittees actively monitored progress by holding over 100 hearings within 4 years to obtain information on the Y2K readiness of federal agencies, states, localities and other important nonfederal entities, such as the securities industry.¹⁰ For example, the House Subcommittee on Government Management, Information and Technology of the Committee on Government Reform held the first congressional hearing on Y2K in April 1996 and developed a report card system for periodically grading agencies on their progress. The Department of Energy reported that high visibility metrics, such as the subcommittee's report cards, got the attention of senior management and motivated performance. In the Senate, the Special Committee on the Year 2000 Technology Problem held numerous hearings on the readiness of key economic sectors, including power, health care, telecommunications, transportation, financial services, and emergency services. Other House and Senate committees and subcommittees also held Y2K hearings. For example, in May 1996, the Subcommittee on Technology of the Committee on Science—co-chair with the Subcommittee on Government Management, Information and Technology of the House Year 2000 Task Force—held a hearing on potential technical solutions and possible roles for the government in addressing the Y2K problem.

⁹S. Res. 208 established the Special Committee on the Year 2000 Technology Problem in April 1998 to study the impact of the Year 2000 problem. This committee disbanded on February 29, 2000.

¹⁰The Congressional Research Service's Y2K Electronic Briefing Book (<http://www.congress.gov/brbk/html/eb/y2k16.html>) provides a complete listing of Y2K hearings.

B-286056

The Congress also passed legislation to facilitate the nation's Y2K work. For example, in October 1998, the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271) was enacted, which provided limited exemptions and protections for the private sector in order to facilitate the sharing of information of Y2K readiness. Early on, Y2K information bottlenecks were widespread in the private sector. According to the President's Council on Year 2000 Conversion's final report, antitrust issues and a natural tendency to compete for advantage made working together on Y2K difficult, if not inconceivable, for many companies. Moreover, according to this report, the threat of lawsuits had companies worried that they would be held liable for anything they said about the Y2K compliance of products or devices they used or the test processes and results for them. The President's Council also noted that legal considerations prevented companies from saying anything about their own readiness for the date change.

According to the President's Council, the Year 2000 Information and Readiness Disclosure Act paved the way for more disclosures about Y2K readiness and experiences with individual products and fixes. Several major telecommunications companies, for example, indicated their willingness to share Y2K information with smaller companies who contacted them. In another example, the leaders of the electric power industry began a series of regional conferences for local distribution companies in which they discussed identified problems and solutions, particularly with embedded chips, as well as testing protocols and contingency planning. The President of the Information Technology Association of America stated that the act allowed businesses to work together more closely to solve issues quickly.

Congressional action continues to be important in addressing key IT issues. For example, during the March through July 2000 time frame, the House Subcommittee on Government Management, Information and Technology, Committee on Government Reform, held nine hearings related to federal IT issues, including a June hearing on the proposed Cyber Security Information Act of 2000, which is intended to remove barriers to information sharing between government and private industry and is modeled after the Year 2000 Information and Readiness Disclosure Act in many respects. Other committees and subcommittees, such as the Senate Committee on Governmental Affairs, have also held recent hearings that address IT issues.

B-286056

**Central Leadership and
Coordination of the Federal
Y2K Effort Was Invaluable**

Actions by the President's Council on Year 2000 Conversion, OMB, and the Chief Information Officers (CIO) Council¹¹ all demonstrated the value of central leadership and coordination. The President's Council focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community. The President's Council's activities fell into three areas: (1) ensuring that federal systems were ready for the date change, (2) coordinating Y2K efforts with interface partners (primarily states) for important federal services, and (3) promoting action on the Y2K problem among businesses and other governments whose failures could have had an adverse effect on the American people. To achieve its mission, the President's Council

- convened Year 2000 summits, in partnership with the National Governors' Association, with state and U.S. territory Year 2000 coordinators in July 1998, March 1999, and October 1999, and participated in monthly, multistate conference calls with state Year 2000 coordinators;
- established a nationwide campaign to promote "Y2K Community Conversations," which were locally based forums to support and encourage the efforts of government officials, business leaders, and interested citizens to share information on their progress; and
- promoted international cooperation on Y2K, working with the United Nations and assisting in the creation of the International Y2K Cooperation Center.

OMB, for its part, played an important role in leading, coordinating, and monitoring federal Y2K efforts. Among its accomplishments, OMB

- directed the major departments and agencies to submit quarterly reports beginning May 15, 1997, in order to monitor individual agency progress;
- designated lead agencies, in March 1999, for the government's 42 (later updated to 43) high-impact programs, such as food stamps, Medicare, and federal electric power generation and delivery; and

¹¹The CIO Council consists of CIOs and deputy CIOs from 30 federal departments and agencies; representatives from OMB; and liaisons to other councils, committees, and boards. It is the principal interagency forum for improving the design, modernization, use, sharing, and performance of IT resources.

B-266056

- clarified its contingency plan instructions in early 1998 and, along with the CIO Council, adopted our Business Continuity and Contingency Guide¹² for federal use.

Several participants in the Y2K Lessons Learned Summit cited the value of the CIO Council. In November 1996, the CIO Council established a Year 2000 Committee,¹³ which met monthly and addressed important issues, such as acquisition and Y2K product standards, data exchange issues, telecommunications, buildings, biomedical and laboratory equipment, and international issues. A particularly important role of the CIO Council was coordinating data exchange issues with the states. For example, it cosponsored federal-state summits with the National Association of State Information Resource Executives to address this key issue. Y2K Lessons Learned Summit participants called for additional support for the CIO Council. One participant at the summit stated that the CIO Council should have staff support and funding.¹⁴

In addition, OMB, the CIO Council, and GAO issued standard guidance that was universally accepted, adopted, and implemented, which facilitated Year 2000 conversion efforts and related oversight. This guidance (1) provided a level of consistency across government by providing standard terms, tools, and techniques based on best practices, (2) imposed structure and discipline, (3) increased the rigor of testing and assessment, (4) promoted consistency in data gathering and reporting, and (5) facilitated evaluation of actions by both agency management and auditors.

We have previously stressed the need for better coordination among federal agencies. In January 1999, we pointed out that virtually all the results that the federal government strives to achieve require the concerted and coordinated efforts of two or more agencies and that in program area after program area we have found that unfocused and uncoordinated crosscutting programs waste funds, confuse and frustrate taxpayers, and limit program effectiveness.¹⁵ Accordingly, the central leadership and

¹²GAO/AIMD-10.1.19, August 1998.

¹³The government's interagency working group on year 2000, established in late 1995, evolved into the CIO Council's Year 2000 Committee.

¹⁴Currently the CIO Council is funded and staffed by individual federal agencies.

¹⁵*Major Management Challenges and Program Risks: A Governmentwide Perspective* (GAO/OCG-99-1, January 1999).

B-256056

coordination that proved valuable during Y2K will continue to be key to effectively addressing major government management issues.

**Value of Partnerships Often
Cited as an Important Y2K
Lesson**

Partnerships between the public and private sector and among federal, state, local, and international entities were key to addressing issues such as data exchanges and the coordination of business continuity planning for entire industrial sectors. Shortly after the President's Council was established, we recommended that it use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.¹⁶ The President's Council subsequently established over 25 sector-based working groups, led by one or more federal entities, that established partnerships with over 250 organizations to gather information critical to the nation's Y2K efforts and to address issues such as contingency planning. These partnerships also paid dividends during the century date rollover period when 11 private sector organizations, designated as National Information Centers, provided information on the status of critical sectors, such as electric power and telecommunications. At the Y2K Lessons Learned Summit, the Chairwoman of the House Subcommittee on Technology, Committee on Science, characterized the partnerships formed to address Y2K as superlative.

To illustrate the importance of these partnerships, the Department of Energy reported that its partnership with the North American Electric Reliability Council enabled it to monitor progress, highlight industry issues requiring the department's assistance, address the industry's privacy and competition issues, and build a positive working relationship that will prove valuable in the future. Further, during the Y2K Lessons Learned Summit, the HCFA Administrator stated that agency staff carried out unprecedented outreach to providers and beneficiaries. According to the Administrator, for the first time, HCFA communicated directly with about 1.2 million Medicare providers, and it plans to continue direct communications with providers on important issues.

Federal-state partnerships were also critical because 10 of the federal programs designated as high impact by OMB are administered by states. The Departments of Agriculture, Health and Human Services, and Labor took action to help states successfully transition these 10 high-impact state-

¹⁶ Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-96-85, April 30, 1996).

administered federal programs into the year 2000. For example, the Department of Agriculture's Food and Nutrition Service obtained a contractor to conduct on-site visits to certain states and territories to provide technical assistance in areas such as software testing and contingency planning.

The President's Council on Year 2000 Conversion also launched several initiatives in the international arena to address Y2K readiness in foreign countries. In particular, the Chair of the President's Council attended National Y2K Coordinators' meetings hosted by the United Nations and was a member of the steering committee of the International Y2K Cooperation Center. Further, through its leadership of the International Relations Working Group of the President's Council, the Department of State worked to increase awareness of the Year 2000 problem throughout the world, collected and shared information on the problem with other federal agencies and foreign nations, and encouraged the remediation of faulty computer systems. Speaking at the Y2K Lessons Learned Summit, the Chairwoman of the House Subcommittee on Technology also cited the air transport industry and the financial sector for their international work.

Like the Y2K problem, the challenge of protecting critical infrastructures from computer-based attacks extends well beyond federal operations. Private sector systems control most of our nation's critical infrastructures, such as energy, telecommunications, financial services, transportation, and vital human services. As a result, establishing public-private partnerships is recognized as one of the major challenges of critical infrastructure protection. Also, as organizations increasingly look to electronic communications and commerce as a means of conducting business, the need for partnerships among federal agencies and other entities is likely to grow in importance. Electronic interdependencies, and the potentially massive exchanges of data that are likely to accompany them, prompt an increasing need for federal agencies and private entities to form partnerships to deal with crosscutting issues, such as Internet service delivery.

While Y2K was a unique and finite challenge, it provided a foundation for establishing relationships that can serve as the beginning of future partnerships. Some organizations are taking steps to continue partnerships. For example, the CIO Council and the National Association of State Information Resource Executives have informally agreed to cooperate on future issues and have formed committees to promote cooperation. Similarly, at the Y2K Lessons Learned Summit, the National Coordinator,

B-286056

Security, Infrastructure Protection, and Counterterrorism, stated that the critical infrastructure protection area was taking the same type of partnership approach that was taken for the Y2K issue. Specifically, the National Coordinator cited the creation of Information Sharing and Analysis Centers, which are intended to facilitate public-private sector information sharing about actual threats and vulnerabilities in individual infrastructure sectors. As of mid-June 2000, two such centers had been established for financial services and telecommunications and several more were expected to be established by the end of the year.

Many Methods Facilitated Communications Among Partners and Others

Effective communication also proved to be a valuable Y2K tool. For example, organizations shared information about the Y2K compliance status of systems, products, and services, and exchanged information about test results and solutions. Federal agencies used many mechanisms to communicate Y2K-related information to partners and others. For example, the Department of Energy (DOE) used a variety of ways to communicate Y2K information to DOE staff and others, including "Awareness Days," a newsletter, and a DOE Y2K web site. The Department of State established an information center as a single point of information for all Y2K status information provided from posts. Because of its effectiveness in consolidating information and avoiding duplication of effort, the Department of State recommended the use of such centers in the future when posts are given new reporting requirements.

The Internet also proved to be a valuable communications channel. The Senate Special Committee on the Year 2000 Technology Problem stated in its final report¹⁷ that use of the Internet provided an unprecedented level of organizational transparency and paved the way for effective public-private partnerships and open communications among different industries preparing for Y2K. According to the Senate report, (1) nearly every business with a presence on the World Wide Web had a link to a statement regarding Y2K compliance and (2) industry groups, associations of public managers, and trade organizations all established web sites. As a result, according to the Senate report, both companies and countries starting late on Y2K work were able to gain enormously from the shared experiences of others. An example of the effective use of the World Wide Web in providing essential Y2K compliance information was the Federal Y2K Biomedical

¹⁷ *Y2K Aftermath—Crisis Averted: Final Committee Report* (U.S. Senate Special Committee on the Year 2000 Technology Problem, February 29, 2000).

B-286056

Equipment Clearinghouse established by the Food and Drug Administration, in conjunction with the Department of Veterans Affairs. According to the Food and Drug Administration, this site received about 317,000 inquiries between April 1998 and September 1999.

In addition to the issue of communicating Y2K status information, the President's Council stated that a major concern was raising awareness about the magnitude of the Y2K challenge without causing overreaction by the public. The President's Council believed that the public would respond appropriately if it had access to information in which it had confidence. Accordingly, the Council adopted a strategy of being transparent in its operations and sharing information readily and in a timely manner. Among the methods the Council used to provide public information were publicizing industry surveys and quarterly assessment reports, establishing a Council web site and a toll-free information line, and holding Y2K community conversations. The President's Council reported that its web site, www.y2k.gov, averaged over 45,000 hits per week, rising to more than 3 million during the century date rollover period, and that its toll-free number averaged 15,000 calls a month. Moreover, during the century and leap day rollover periods, the Chair of the President's Council held over 10 press conferences to convey status reports to the public.

In commenting on a draft of this report, OMB noted the value of the President's Council on Year 2000 Conversion's approach in openly sharing Y2K information with the public. OMB added that because the Y2K problem affected all federal agencies as well as all states and most private-sector organizations, sharing best practices and other technical information was quite helpful.

B-286056

In the future, agencies expect to continue using technology to facilitate communication. For example, the General Services Administration found that the International Virtual Y2K Conference, developed to increase awareness and facilitate the exchange of information between countries, can be used as a model to provide convenient, cost-effective, interactive forums 24 hours a day, 7 days a week. The development of effective communication mechanisms will be essential to the success of critical infrastructure protection. In July testimony, we outlined some of the formidable challenges facing the federal government in this area, including ensuring that the right type of data is collected and that there are effective and secure mechanisms for collecting, analyzing, and sharing it.¹⁸

Human Capital and Budget Initiatives Were Important

In April 1998, we noted that some agencies were reporting problems obtaining and retaining personnel with the technical expertise needed to accomplish Year 2000 conversions.¹⁹ Accordingly, we recommended that the President's Council develop a personnel strategy that would include reemploying former federal employees and identifying ways to retain key Year 2000 staff.

In October 1998, we reported that several efforts had been undertaken to address these workforce issues.²⁰ Some of these efforts illustrate the types of creative solutions that can be considered to solve specific personnel problems. Others serve as a basis for further improvements that could benefit critical infrastructure protection, as well as other information technology management issues.

In particular, the Office of Personnel Management publicized existing tools for retaining staff and supplemented these with additional aids. For example, the Office of Personnel Management

- provided authority to reemploy federal retirees to work specifically on the Year 2000 conversion without the usually required reduction in the retiree's salary or military annuity;

¹⁸Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Strategy and Coordination (GAO/T-AIMD-00-268, July 26, 2000).

¹⁹GAO/AIMD-98-85, April 30, 1998.

²⁰Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1999).

B-286056

- encouraged agency heads to exercise their authority to make exceptions to limitations on premium pay (including overtime, night, and holiday pay) for employees performing emergency work to resolve computer system problems associated with Y2K that posed a direct threat to life and property;
- allowed agencies, in certain circumstances and with Office of Personnel Management approval, to exclude critical Y2K positions from voluntary early retirement programs; and
- allowed agencies to authorize a retention allowance of up to 10 percent of an employee's rate of basic pay (or up to 25 percent with Office of Personnel Management approval) for a group or category of employees such as computer programmers and system engineers that meets certain criteria, for example, being likely to leave federal service in the absence of the allowance.

These tools proved helpful. For example, the Department of the Treasury stated that personnel resources were initially a major hurdle, especially for the IRS. According to the Department of Treasury, IRS was able to overcome this hurdle largely through the government's incentives for retaining personnel.

In commenting on a draft of this report, OMB noted that the "heroes" of the Y2K effort were the technicians who worked long and hard implementing fixes to and testing thousands of systems. It added that these dedicated employees and contractors were willing to go beyond their normal duties and responsibilities to tackle the problem. In addition, OMB pointed out that products were developed by the information technology marketplace to partially automate solutions to the Y2K problem. As a result, according to OMB, these products improved worker productivity and negated the concern regarding having a shortage of technicians to correct code.

Although the Y2K challenge is over, human capital is a continuing issue of major proportions facing federal managers, especially in the IT arena. Serious concerns are emerging about the aging of the federal workforce, the rise in retirement eligibility, the effect of selected downsizing and hiring freeze initiatives, and the actions needed to ensure effective workforce and succession planning for the future. The skills, needs, and imbalances of the workforce, as well as agencies' approaches to managing incentives and performance, all need greater attention than they have been given. Further, human capital decisions in the federal sector are often constrained compared to the flexibility found elsewhere. With respect to IT, at the Y2K Lessons Learned Summit, the Chairman of the Senate Special Committee

B-286056

emergency funding for Year 2000 conversion activities. According to the President's Council on Year 2000 Conversion's final report, OMB reviewed agency requests for this funding and, after its approval, the Congress had 15 days to consider the proposed expenditures. The President's Council report also stated that agencies used the funds for Year 2000 remediation and testing and other important Y2K activities, such as contingency planning.

The Chair of the President's Council on Year 2000 Conversion stated that the availability of the contingent emergency funding was of great assistance to agencies during the last 15 months of their conversion efforts, allowing them to fund Y2K conversion needs discovered late in the process. The Department of the Treasury also cited funding as the major hurdle it faced throughout the Year 2000 challenge, and stated that it would not have been successful in achieving Year 2000 compliance for some of its critical business processes and systems without these emergency funds and the ability to reallocate the department's resources.

Ensuring adequate funding will continue to be an issue in addressing critical infrastructure protection and computer security. For example, according to January 2000 testimony by the Department of State's CIO, who is also the Chairman of the CIO Council's Subcommittee on Critical Infrastructure Protection, one of the key obstacles preventing agencies from immediately pursuing critical infrastructure protection initiatives is the lack of current funding for these projects. Also, in February 2000, we reported that while funding for security is embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance, some additional amounts are likely to be needed to address specific weaknesses and new tasks.²³ Participants in the Y2K Lessons Learned Summit, including the National Coordinator, Security, Infrastructure Protection, and Counterterrorism, also noted that enhancing IT security will require significant expenditures.

²³GAO/T-AIMD-00-72, February 1, 2000.

B-286056

Agency Y2K Efforts Resulted in Improved Information Technology Management

The Year 2000 problem resulted in many agencies taking charge of their information technology resources in much more active ways than they had in the past. We reported in October 1999 that addressing the Year 2000 problem highlighted the importance of good information technology management.²⁴ Moreover, Y2K Lessons Learned Summit participants and agency documents identified specific management practices that could usefully be carried forward to other challenges. These are

- high-level management attention,
- risk analysis,
- project management,
- systems inventories and configuration management,
- independent reviews,
- testing, and
- business continuity and contingency plans.

Agency Y2K Actions Benefited From High-level Management Involvement

The Y2K challenge demonstrated that rather than leaving technology issues to mid-level specialists, agency heads must incorporate strategic information management into an executive-level general management framework. While the Year 2000 problem was technical in nature, it was primarily a management problem, with organizations facing the risk of disruptions of their core business processes. Y2K Lessons Learned Summit participants and agencies cited high-level leadership and top management involvement as key to Y2K success. For example, the Environmental Protection Agency cited as a Y2K lesson that senior management needs to be involved in information technology on an ongoing basis, since IT is at the core of how program offices and regions conduct their business.

²⁴Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-1, October 1, 1999).

HCFA and FAA are prime examples of how strong leadership was able to overcome slow starts in addressing the Y2K problem. With respect to HCFA, in May 1997 and September 1998, we highlighted concerns and made recommendations to improve its Medicare Y2K program.²⁵ As we testified in February 1999, HCFA was responsive to our recommendations, and its top management was actively engaged in its Y2K program.²⁶ Specifically, HCFA's Administrator made compliance the agency's top priority and directed a number of actions to more effectively manage the project. As a result, Medicare was reported to have experienced few Year 2000-related events that affected operations during the century change rollover.

With respect to FAA, in January 1998, we reported that the agency was severely behind in its Y2K work. FAA had no central Y2K program management; an incomplete inventory of mission-critical systems; no overall strategy for renovating, validating, and implementing mission-critical systems; and no milestone dates or schedules.²⁷ In response to our recommendations, the agency established a strong Y2K program office and tasked it with providing leadership—guidance and oversight—for FAA's business lines and aviation industry partners. By September 1999 FAA had made excellent progress in its Year 2000 readiness.²⁸ While FAA's air traffic control system did experience some Year 2000-related problems, none affected safety, service, or capacity, according to FAA.

²⁵ *Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses* (GAO/AIMD-97-78, May 16, 1997) and *Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy* (GAO/AIMD-98-284, September 28, 1998).

²⁶ *Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk* (GAO/T-AIMD-99-89, February 24, 1999).

²⁷ *FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically* (GAO/AIMD-98-45, January 30, 1998).

²⁸ *Year 2000 Computing Crisis: FAA Continues to Make Important Strides, But Vulnerabilities Remain* (GAO/T-AIMD-99-285, September 9, 1999).

B-286056

DOD also recognized the importance of senior-level management in its Year 2000 effort. According to its lessons learned report, in the summer of 1998, senior DOD leaders recognized that Y2K was a "chief executive officer" problem. As a result, in August 1998 the Secretary of Defense directed DOD leadership to treat the Year 2000 issue as a major threat to military readiness. According to DOD, this was a turning point and it ensured that all members of DOD understood the necessity of cooperation to achieve success in preparing for Y2K and galvanized preparedness activities. In September 1999, DOD announced its intention to develop a "Y2K like" approach for tracking and reporting Chief Financial Officer compliance of its financial management systems. We testified in July that the department had learned through its Y2K effort that major initiatives that cut across DOD components, such as financial management, must have the leadership of the Secretary and Deputy Secretary of Defense to succeed.²⁹ Our survey of leading financial management organizations also stressed the importance of strong leadership from top leaders.³⁰

Continuing to view IT as integral to achieving an agency's mission is essential to future success in developing systems that meet management needs. Executives of leading organizations no longer regard technology management as a separate support function and instead strive to understand how information management investments are made and how they integrate with other investments and the overall business vision. As a result, CIOs typically serve as a bridge between top managers, information management professionals, and end users.³¹ According to HCFA's CIO, Y2K helped break down internal organizational barriers and facilitated bridge-building and communication. In other examples, the Postal Service reported that Y2K strengthened cross-functional relationships, which it stated would facilitate cooperation on other large-scale projects and the U.S. Customs Service reported that its Y2K program served as a catalyst to improve communications within its IT office, as well as with other areas of the agency.

²⁹Department of Defense: *Implications of Financial Management Issues* (GAO/T-AIMD/NSIAD-00-264, July 20, 2000).

³⁰Executive Guide: *Creating Value Through World-class Financial Management* (GAO/AIMD-00-134, April 2000).

³¹Executive Guide: *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, Exposure Draft (GAO/AIMD-00-83, March 2000).

**Risk Analysis Allowed
Agencies to Prioritize Work**

According to officials involved in the Year 2000 conversion, the Year 2000 challenge has served as a wake-up call to many who were previously unaware of our nation's extensive dependence on computers. This new awareness of the importance of computer systems and of their vulnerabilities can serve as a basis for better understanding long-term risks to computer-supported critical infrastructures. Year 2000 preparations also forced agencies to identify those systems that were mission-critical.

Agencies used risk analyses to help direct their Y2K actions. For example, in testing interfaces between its own systems and with external business partners, the Department of Housing and Urban Development first listed, described, and analyzed its interfaces, then ranked them based upon risk. High-risk interfaces and those with external partners were then tested in both current and forward date environments.

Risk analysis will be an important part of security planning. OMB Circular A-130 requires agencies to consider risk when deciding what security controls to implement. It states that a risk-based approach is required to determine adequate security, and it encourages agencies to consider major risk factors. The National Institute for Standards and Technology and we have issued guidance on risk assessment.³² Earlier this year, we testified on the need for governmentwide risk-based standards for information systems controls, which would assist agencies in ensuring that their most critical operations and assets are protected at the highest levels while providing agencies the flexibility to apply less rigorous controls to lower risk operations and assets.³³

³²*An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, December 1995; *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996; and *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).

³³GAO/T-AIMD-00-72, February 1, 2000.

B-286056

Improved Project Management Practices Were Implemented

Effective project management is key to developing and implementing successful IT projects. Our IT investment management guides emphasize the importance of project management and oversight in helping to ensure that IT projects are kept on schedule and within budget.³⁴ In addition, our best practices guide *Improving Mission Performance Through Strategic Information Management and Technology* points out that instituting a performance measurement program can improve information systems' contribution to mission outcomes.³⁵

One benefit of the Y2K effort that could have lasting effects is the new, improved monitoring practices and performance metrics that several agencies reported that they had implemented. Examples include the following:

- The Commissioner of the U.S. Customs Service committed to leveraging the agency's Year 2000 experience by extending the level of project management discipline and rigor being employed on the year 2000 to other information programs and projects.
- The Department of Housing and Urban Development reported that it strengthened its IT management by developing an Integrated Implementation Plan that tracks progress and views interdependent relationships between information system development efforts. According to the department, the plan now tracks all of its development initiatives.
- The Department of State reported that it developed eight products and processes related to tracking and reporting progress with potential value beyond Y2K. These included standard management indicators, regular reporting cycles, and a "war room" (an operations center-like structure capable of maintaining all project indicators, quickly responding to status requests, and serving as the central hub for information management and reporting).

³⁴*Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Exposure Draft (GAO/AIMD-10.1.23, May 2000) and *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making* (GAO/AIMD-10.1.13, February 1997).

³⁵*Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology* (GAO/AIMD-94-115, May 1994).

Improved Inventories and Configuration Management

According to the Chair of the President's Council, prior to the Y2K problem, no federal agency had a complete IT inventory. However, the Y2K issue forced agencies to develop inventories as part of their remediation, and many agencies consider these inventories valuable assets. For example, the Environmental Protection Agency (EPA) reported that the Y2K project provided program offices and regions a comprehensive and current inventory of their IT infrastructure (e.g., hardware, software, and licenses) and processes. As a result, EPA has asset information by organization, which was not previously available. Similarly, the Department of Housing and Urban Development reported that it created several reusable repositories of information, such as an inventory of systems, their interrelationships, and their relationships with external business partners. The Department of Housing and Urban Development reported that it now has a much better high-level view of these relationships and has already used the documentation for several departmentwide initiatives. The International Y2K Cooperation Center pointed out the value of comprehensive inventories in managing large-scale projects. The center reported that knowledge about systems and suppliers fed into a broader understanding within organizations about how they perform their missions.

Improved configuration management³⁶ also resulted from agencies' Y2K work. Weak applications software development and change controls³⁷ are repeatedly highlighted in our reviews of federal agencies.³⁸ Without these controls, individuals can surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage. However, as a result of their Y2K efforts, agencies have reported new or strengthened configuration management practices. For example, the Department of State reported that as a result of its Y2K work, it has change control and configuration management plans that contain information about change control boards, change requests, change approval, documentation control, and version control. The

³⁶Configuration management is defined as the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

³⁷Software development and change controls prevent unauthorized software programs or modifications to programs from being installed.

³⁸We recently reported on the software controls at 16 agencies. The aggregate results of our work were reported in *Information Security: Controls Over Software Changes at Federal Agencies* (GAO/AIMD-00-151R, May 4, 2000).

B-286056

Department of State expects that these plans will be useful for tracking future application changes and consolidating change management procedures. DOD and EPA report that they too have instituted improved configuration management processes following their Y2K experiences.

Independent Reviews Provided Valuable Management Information

Independent reviews proved to be an important mechanism for monitoring Y2K progress and uncovering problems that needed attention. Y2K Lessons Learned Summit participants and agencies reported that both auditors' reviews and independent validation and verification (IV&V) work were valuable in preparing for the year 2000. For example, DOD's inspector general and military service internal auditors issued more than 200 reports on Y2K progress. A summary report issued by the DOD Inspector General in December 1999 lists numerous DOD actions taken in response to its recommendations.³⁹ Accordingly, DOD reported that auditing was a major factor in its Y2K success. The HCFA Administrator similarly cited the value of work done by the Department of Health and Human Services Office of the Inspector General and IV&V vendors at contractor sites in uncovering problems.

Moreover, two agencies specifically cited IV&V as having future value. The U.S. Customs Service stated that two aspects of its Y2K IV&V program—an automated tool to uncover data anomalies and the use of agencywide teams to review procedures—will continue. The Department of Energy found the use of IV&V “extremely beneficial,” especially in the area of independent source code verification, and recommended the use of independent verification of software code to find all source code errors, not just those that were Y2K-related.

Y2K Work Led to Development of Reusable Testing Practices

An effective testing program was an essential component of any Year 2000 program or project. Accordingly, as part of their Y2K activities, agencies implemented testing practices and developed test procedures that should continue to be useful. In November 1998 we issued a Y2K testing guide⁴⁰ that laid out a disciplined approach to testing activities that are hallmarks

³⁹Summary of DOD Year 2000 Issues IV (Office of the Inspector General, Department of Defense, Report No. D-2000-057, December 16, 1999).

⁴⁰GAO/AIMD-10.1.21, November 1998.

B-286056

of mature software and systems development/acquisition and maintenance processes.

During the Y2K process, agencies acted to address the criteria in this guide. For example, in October 1999 we reported that the Department of the Treasury's Financial Management Service had established the 11 key organizational infrastructure processes that our test guide defined and had satisfied the key end-to-end testing processes specified in the guide.⁴¹ The Department of State reported that its test plans contained scripts and scenarios for both Y2K and non-Y2K testing, as well as information on the testing environment and the tools used. The department expects that these plans can be used as the basis for future application testing.

DOD in particular performed extensive Y2K testing. It reported conducting 36 operational evaluations, 31 major end-to-end tests, and 56 large-scale systems integration tests. These tests involved thousands of individuals and systems worldwide. DOD also used a technique called "thin line systems analysis" to determine the critical paths by which information flowed during the execution of primary missions. The identification of these "thin lines" allowed DOD to identify all mission-critical systems for each DOD mission/function. These systems were then included in end-to-end testing to ensure that all elements were fully Y2K compliant. According to the DOD lessons learned report, in the future, the department will incorporate information assurance, critical infrastructure protection, interoperability, and configuration management issues into routine exercise and training programs.

Business Continuity and Contingency Plans Were Beneficial

Business continuity and contingency planning was necessary to reduce the risk and potential impact of possible Y2K failures, and this planning proved its value during the Y2K rollover. For example, a "zero day" test of the DOE Oak Ridge facility's Dynamic Special Nuclear Material Control and Accountability System found a Year 2000-related file transfer error. After the rollover, one segment of the software began generating file identifiers with a four-digit year format, while the file transfer software was expecting a two-digit year format. As a result, the test of the transfer failed. According to DOE, contingency plans that had been updated and tested because of the Year 2000 problem were implemented and magnetic tapes were used to

⁴¹ Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls (GAO/AIMD-00-24, October 29, 1999).

B-286056

successfully transfer the information. The failure was corrected a short time later.

Agencies' business continuity and contingency plans developed for Y2K, as well as the planning process itself, will have continuing benefits. Agencies found that in developing Y2K contingency plans, they developed processes that will help deal with future issues. For example, the Department of Housing and Urban Development reported that its contingency planning process generated a better understanding of its business and the interdependencies among program areas. The Department of State has reported that it derived a methodology, information, and tools from the contingency planning process with potential value beyond Y2K. The department noted that plans were developed for the business processes supported by IT systems and that these contingency plans apply to any failure the system might experience.

In assessing the value of its Y2K contingency planning process for the future, the Nuclear Regulatory Commission found that it bolstered its continuity of operations plan and improved its capability to communicate with federal, state, and licensee decisionmakers. The Nuclear Regulatory Commission also stated that it was better prepared to respond to multiple simultaneous events. Moreover, it plans to pursue (1) continuing the use of communications procedures with other federal agencies that were established for Y2K and (2) developing an Internet-based reporting system similar to what it developed for Y2K for sharing International Nuclear Event Scale reports.

Sustaining Y2K Momentum Is Critical to Achieving Success in Other Management Challenges

Although the American people expect world-class public services and are demanding more of government, the public's confidence in the government's ability to address its demands remains all too low. Yet, Y2K demonstrated that strong federal leadership can effectively tackle a major management challenge and yield positive results. If the government successfully sustains the momentum from its Y2K victory as it turns to other major management challenges of the new century, the government may begin to earn back the public's confidence.

B-286056

As we reported in April 1998, while the Year 2000 problem had the potential to be catastrophic, the very real risks could be mitigated and disruptions minimized with proper attention and management.⁴² At that time, we also noted that the recently established President's Council provided an opportunity for the executive branch to take key steps to avert disruptions to critical services, serving as the linchpin that bridged the nation's and the federal government's various Y2K initiatives. This is indeed what happened as the President's Council, under the leadership of the Chair, ably assumed the Y2K leadership mantle.

The momentum generated by the government's Y2K success provided an opportunity to improve the government's use of information technology to modernize services and thus achieve results, which we have identified as a major challenge agencies face in becoming high-performance organizations.⁴³ In particular, the government must effectively address the following areas: critical infrastructure protection and security, the effective use of technology, and large-scale IT investments.

- **Critical infrastructure protection and security.** Computer security risks have increased dramatically over the last decade as our government and our nation have become ever more reliant on interconnected computer systems to support critical operations and infrastructures. While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. In February 2000, we testified that the government is not adequately protecting critical federal operations and assets.⁴⁴

⁴²GAO/AIMD-98-85, April 30, 1998.

⁴³*Managing in the New Millennium: Shaping a More Efficient and Effective Government for the 21st Century* (GAO/T-OCG-00-9, March 29, 2000).

⁴⁴GAO/T-AIMD-00-72, February 1, 2000.

Computer viruses and other types of computer attacks are also a continuing threat. The National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack them. According to DOD officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. According to a leading security software designer, viruses in particular are becoming more disruptive for computer users. The Melissa and "ILOVEYOU" viruses illustrated the potential disruption such attacks can cause. As we have testified, while key government services remained largely operational during these attacks, these viruses were disruptive and provided evidence that computer attack tools and techniques are becoming increasingly sophisticated.⁴⁵

- **Effective use of technology.** Electronic commerce and business strategies made possible by widespread Internet access and interconnected systems are transforming how organizations, both public and private, will operate in the next decade. Governments at all levels are using the Internet and other means of electronic commerce to improve internal business operations and to provide on-line public access to information services. However, for the most part, federal, state, and local governments are in the early stages of shifting their perspective to citizen-centered services and are just beginning to move toward the real potential of e-government.

As we noted in May 2000, top leadership must effectively merge the power of electronic interactions—among agencies, with businesses, and with the public—with necessary and corresponding management and process improvements that will better ensure positive outcomes.⁴⁶ For example, an immediate and complex leadership challenge confronting government policymakers and managers is the need to adopt informed strategies to guide agencies in how best to use the Internet to deliver services to all citizens and business partners.

⁴⁵For example, *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (T-AIMD-99-146, April 15, 1999) and *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000).

⁴⁶*Electronic Government: Federal Initiatives Are Evolving Rapidly But They Face Significant Challenges* (GAO/T-AIMD/GGD-00-179, May 22, 2000).

B-286056

Another challenge is the government's ability to address privacy concerns. It is no longer technically difficult for the government to establish databases that collect extensive personal information about large numbers of individual citizens. Individuals should be able to determine when, how, and to what extent this personal information is collected and used. However, if not properly implemented and managed, the technologies that have been developed to manage massive volumes of personal information could also be abused. For example, in May 2000 we reported⁴⁷ that the Social Security Administration had been cautious in pursuing its on-line initiatives largely because of the privacy and security concerns raised following its implementation of the on-line personal earnings and benefits estimate statement.⁴⁸

- **Large-scale IT investments.** As we testified in March, federal agencies invest about \$38 billion to build, operate, and maintain automated systems each year.⁴⁹ If managed effectively, these investments can vastly improve government performance and accountability. If not, however, they can result in wasteful spending and lost opportunities for improving delivery of services to the public.

Agencies are now beginning to address new IT investment needs that were deferred because of their recent, and appropriate, focus on the Year 2000 conversion. As a result, we anticipate that they will undertake major modernization programs and large-scale IT projects in the very near future, making the need for fundamental improvements in the way agencies manage IT investments even more urgent. While some agencies are making tangible improvements in managing large-scale IT investments, many are still in the beginning stages and more needs to be done.

⁴⁷Social Security Administration: Subcommittee Questions Concerning Current and Future Service Delivery Challenges (GAO/AIMD/HEHS-00-165R, May 11, 2000).

⁴⁸The Social Security Administration's on-line personal earnings and benefits estimate statement initiative was later put on hold. See *Social Security Administration: Information Technology Challenges Facing the Commissioner* (GAO/T-AIMD-98-109, March 12, 1998) and *Social Security Administration: Internet Access to Personal Earnings and Benefits Information* (GAO/T-AIMD/HEHS-97-123, May 6, 1997).

⁴⁹GAO/T-OCG-00-9, March 29, 2000.

B-286056

The government has had problems effectively addressing these major information technology issues. For example, recent audits conducted by us and by agency inspectors general show that 24 of the largest federal agencies have significant computer security weaknesses, including poor controls over access to sensitive systems and data, poor controls over software development and changes, and nonexistent or weak continuity of service plans.⁵⁰ Further, to be successful, e-government initiatives must overcome some of the basic challenges that have plagued information systems for decades—inadequate attention to technical and business architecture, adherence to standards, and security. With respect to major IT investments, during the 1990s we issued many reports that documented billions of dollars in wasted IT expenditures for computer systems that failed to deliver expected results and poorly defined management processes that fostered suboptimal solutions to agency business needs.

Strong and effective governmentwide leadership can make a difference in addressing these types of issues. Effective top management leadership, involvement, and ownership are the cornerstone of any IT investment strategy. As we testified in July 2000, strong leadership will be required to develop and implement a comprehensive and cohesive strategy to ensure that our information security and critical infrastructure protection efforts are effective.⁵¹ In particular, because of the number of entities involved in critical infrastructure protection,⁵² leadership will be essential to ensuring that their efforts are coordinated and adequately communicated to individual agency personnel and that critical infrastructure efforts are appropriately linked with broader computer security work. Finally, top-level leadership is also important to ensuring that the key Y2K lessons, such as the importance of partnerships, communications, and human capital and funding, are preserved.

⁵⁰Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies (GAO/AIMD-00-295, September 6, 2000).

⁵¹GAO/T-AIMD-00-268, July 26, 2000.

⁵²Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including OMB, the National Institute for Standards and Technology, and the National Security Agency. Other organizations are also becoming involved in the administration's critical infrastructure protection initiative, including the Department of Justice and the Critical Infrastructure Assurance Office.

The Congress is considering the need for legislation to provide strong and effective central information resources and technology management leadership. In particular, although they differ in approach, three bills⁵³ embrace the need for a central focus point to provide effective federal government IT leadership.

We have long called for strengthened central information resources and technology management through the creation of a formal CIO position for the federal government.⁵⁴ The creation of a CIO for the federal government could provide a strong, central point of coordination for the full range of governmentwide information resources management and technology issues, including (1) reengineering and/or consolidating interagency or governmentwide process and technology infrastructure, (2) managing shared assets, and (3) evaluating high-risk, complex information systems modernization efforts.

As we previously discussed, the leadership of the Chair of the President's Council on Year 2000 Conversion was invaluable in combating the Year 2000 problem. Under the Chair's leadership, the government's actions went beyond the boundaries of individual programs or agencies and involved governmentwide oversight, interagency cooperation, and cooperation with partners, such as state and local governments, the private sector, and foreign governments. A federal CIO could maintain and build upon these actions in leading the government's future IT endeavors. Moreover, a federal CIO could adopt other Y2K lessons, such as updating and developing IT management policy and standards in areas such as security and e-government.

Consensus has not been reached on the need for a federal CIO. At our Y2K Lessons Learned Summit, the Chairman of the Senate Special Committee on the Year 2000 Technology Problem stated that a federal CIO was needed, but other participants did not agree or were uncertain about whether a

⁵³The Government Information Security Act (S. 1993), the Chief Information Officer of the United States Act of 2000 (H.R. 4670), and the Federal Information Policy Act of 2000 (H.R. 5024).

⁵⁴*Improving Government: Actions Needed to Sustain and Enhance Management Reforms* (GAO/T-OCG-94-1, January 27, 1994), *Government Reform: Using Reengineering and Technology to Improve Government Performance* (GAO/T-OCG-95-2, February 2, 1995), *Government Reform, Legislation Would Strengthen Federal Management of Information and Technology* (GAO/T-AIMD-85-205, July 25, 1985), and *Information Security: Comments on Proposed Government Information Act of 1999* (GAO/T-AIMD-99-107, March 2, 2000).

B-286056

federal CIO was needed. Further, in response to a question on the need for a federal IT leader accountable to the President asked during a hearing before the House Subcommittee on Government Management, Information, and Technology, the Director of OMB stated that OMB's Deputy Director for Management, working with the head of OMB's Office of Information and Regulatory Affairs, can be expected to take a federal IT leadership role. The Director voiced his concern that if the CIO function were split from OMB, resources would have to be built up in this new organization that would mirror OMB's resources. Finally, the Director stated that he believed that "the right answer is to figure out how to continue to use the authority and the leadership responsibilities at the Office of Management and Budget to play a lead role in this [IT] area."

Our primary concern regarding an OMB official, such as the Deputy Director for Management or the head of the Office of Information and Regulatory Affairs, serving in the role of the federal CIO is whether the official can devote sufficient full-time focus, attention, and energy to governmentwide information resources and technology management leadership, policy, and oversight. Currently, in addition to their information resources and technology management responsibilities, both the Deputy Director for Management and Administrator of the Office of Information and Regulatory Affairs have many other important duties, which necessarily restrict the amount of attention that they can give to these issues. For example,

- The Deputy Director for Management coordinates and supervises a wide range of general management functions, including those relating to managerial systems, such as the systematic measurement of performance; procurement policy; regulatory affairs; and other management functions (e.g., organizational studies, long-range planning, program evaluation, and productivity improvement).
- The Office of Information and Regulatory Affairs, which reports to the Deputy Director for Management, reviews agency proposals for new or revised federal regulations and information collection requirements. For example, the office acts on 3,000 to 5,000 information collection requests from agencies per year, reviews about 500 proposed and final rules each year, and is responsible for calculating the costs and benefits of all federal regulations.

B-286056

We believe that a federal CIO, like agency CIOs, should be primarily concerned with information resources and technology management. Indeed, as we testified in October 1997, OMB itself has raised concerns about agencies in which the CIOs had other major management responsibilities or in which it was unclear whether the CIOs' primary duty was the information resource management function.⁵⁸ Concerns such as these can only be magnified in the case of a federal CIO, whose responsibilities would be far broader than an agency CIO's.

Another concern is whether OMB has sufficient expertise to execute the myriad responsibilities that would be expected of a federal CIO. For example, in an April hearing before the House Subcommittee on Government Management, Information, and Technology, OMB's Director stated that the Office of Information and Regulatory Affairs has a wide range of responsibilities and is "a very heavily worked division."

Conclusions

The challenges associated with the Year 2000 date conversion exemplify the broader and longer-term challenges that our nation faces in managing and protecting elements of our computer-supported critical infrastructure. Consequently, lessons learned in managing the Y2K effort can provide valuable insights to help the federal government invest wisely in future IT projects and provide a secure IT environment. Moreover, some of the concepts used to address the Y2K challenge, such as the importance of leadership and using disciplined processes, have applications even beyond IT to a broad range of management reforms. Many of the efforts undertaken to manage and remedy the Year 2000 problem have resulted in reusable plans, processes, or inventories that can be applied to these longer-term challenges. However, continuity of focused leadership at a governmentwide level has not been sustained in the same fashion. As the federal government moves to fully embrace the digital age and focuses on electronic government initiatives, such comprehensive and focused leadership is of paramount importance.

⁵⁸ *Chief Information Officers: Ensuring Strong Leadership and an Effective Council* (GAO/T-AIMD-98-22, October 27, 1997).

B-286056

Matter for Congressional Consideration

To improve federal government information resources and technology management, address emerging issues, such as e-government, and sustain the focused attention that was developed to address the Year 2000 challenge, the Congress should consider establishing a formal Chief Information Officer position for the federal government to provide central leadership and support. A federal Chief Information Officer could bring about ways to use IT to better serve the public, facilitate improving access to government services, and help restore confidence in our national government. With respect to specific responsibilities, a federal CIO could be responsible for key functions, such as developing information resources and technology management policies and standards; overseeing federal agency IT activities; managing crosscutting issues; ensuring interagency coordination; serving as the nation's chief IT spokesman internationally; and maintaining appropriate partnerships with state, local, and tribal governments and the private sector.

Agency Comments and Our Evaluation

In commenting on a draft of this report, OMB agreed that leadership, coordination, communications, human capital, and funding were keys to the government's Y2K success. OMB also agreed that agencies should take maximum advantage of the benefits derived from Y2K. OMB added that it believed two other Y2K lessons were noteworthy—the dedication of federal employees and contractors and an IT marketplace that moved rapidly to address problems. It also emphasized the value of openness—sharing best practices and sharing information with the public—which we address in the report.

We acknowledge that there may be other Y2K lessons learned. Our report highlights key lessons that were brought up by the attendees at the Y2K Lessons Learned Summit from the executive and legislative branches and the private sector, as well as those documented by agencies that can be utilized in addressing other IT challenges. We added to the report, as appropriate, the lessons noted by OMB.

In further commenting on the draft, OMB agreed that the momentum generated by the Y2K success can be helpful in addressing the three IT challenges we address in the report (critical infrastructure and security, effective use of technology, and large-scale IT investments). However, OMB also pointed out that it believed that Y2K was a finite problem with a fixed deadline and, as such, was much simpler to address than other key IT management challenges such as security, which involves a rapidly changing

technical threat. Moreover, OMB stated that Y2K did not require an investment in research and development for the longer term, as the Administration has proposed to address critical infrastructure protection and security issues. It concluded that the approach that worked to address the Y2K problem may or may not be the most effective one for addressing other IT challenges.

We agree that Y2K was a unique and finite management challenge. Nevertheless, as we discuss in the report, many of the approaches taken to address the Y2K problem can be used to confront other governmentwide IT management challenges. In particular, central leadership, namely the Chair of the President's Council on Year 2000 Conversion, was effective in addressing the problem and played a pivotal role in the government's success. Just like Y2K, the other IT challenges discussed in our report will require sustained and focused leadership to be resolved. For example, regarding critical infrastructure protection, because of the number of entities involved, leadership will be essential to ensuring that efforts are (1) coordinated and adequately communicated to individual agency personnel and (2) appropriately linked with broader computer security work. In the case of e-government, a CIO could (1) help set priorities for the federal government, (2) ensure that agencies consider interagency web site possibilities, including how best to implement portals or central web access points that provide citizens access to similar government services, and (3) help establish funding priorities, especially for crosscutting e-government initiatives.

Regarding our matter for congressional consideration, OMB reiterated its position that it does not support the establishment of a new office for a federal CIO. According to OMB, the Administration believes that the requisite authorities within such an office are already vested in the Deputy Director for Management. OMB pointed out that the President's Council on Year 2000 Conversion was focused on a single issue for a finite period of time and that the Chair was not a CIO.

While the role and responsibility of a federal CIO would likely be broader than that of the Chair of the President's Council, many of the characteristics of this position that proved effective could be carried forward by a federal CIO. For example, a federal CIO, like the Chair of the President's Council, could provide full-time focus and attention to a specific issue, namely information resources and technology management. As we discuss in the report, our primary concern with OMB's role in this area is that the Deputy Director for Management and the Office of

B-286056

Information and Regulatory Affairs have many other important duties that limit the time and attention that can be devoted to information resources and technology management. Moreover, like the Chair of the President's Council, a federal CIO could use his/her position to look beyond the boundaries of individual programs or agencies and provide governmentwide oversight and promote interagency cooperation and cooperation with partners, such as state and local governments, the private sector, and foreign governments.

We are sending copies of this report to Senator Fred Thompson, Chairman, and Senator Joseph I. Lieberman, Ranking Minority Member, Senate Committee on Governmental Affairs; Senator Robert F. Bennett and Senator Christopher J. Dodd, former Chairman and Ranking Minority Member of the Senate Special Committee on the Year 2000 Technology Problem; Representative Jim Turner, Ranking Minority Member, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform; and Representative Constance A. Morella, Chairwoman, and James A. Barcia, Ranking Minority Member, Subcommittee on Technology, House Committee on Science. In addition, we are providing copies to the Honorable Jacob J. Lew, Director, Office of Management and Budget; the participants in the Y2K lessons learned conference listed in appendix II; and other interested parties. Copies will also be made available to others upon request.

If you have any questions on matters discussed in this report, please contact me at (202) 512-6253 or by e-mail at willemsenj.aimd@gao.gov. Key contributors to this assignment were Linda Lambert and Glenn Spiegel.

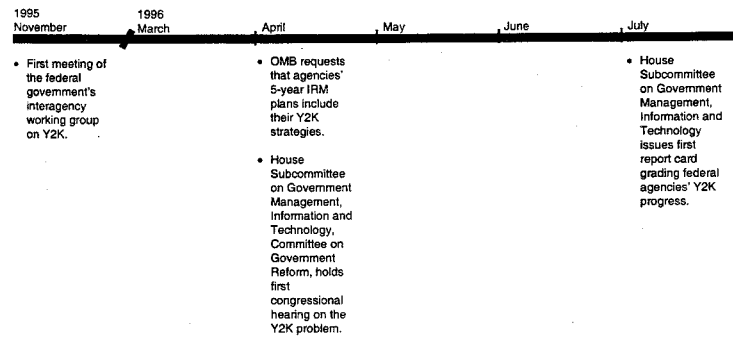
Sincerely yours,



Joel C. Willemsen
Director, Civil Agencies Information Systems

Appendix I

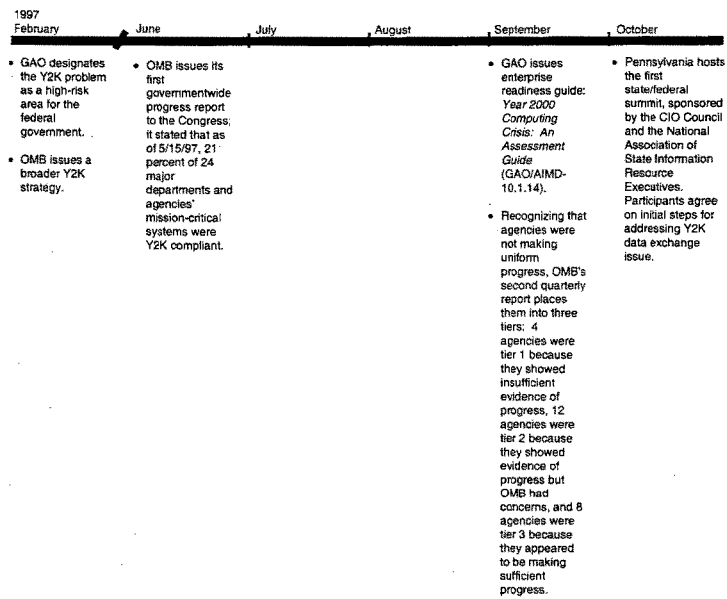
Timeline of Major Y2K Events



Appendix I
Timeline of Major Y2K Events

August	September	October	November	December	1997 January
			<ul style="list-style-type: none"> Interagency working group evolves into CIO Council's Year 2000 Committee, with two objectives: reemphasizing IT practices to ensure that mission-critical systems work on, before, and after 1/1/00 and identifying joint efforts to leverage resources for solving the Y2K problem. 		<ul style="list-style-type: none"> Federal Acquisition Regulation Council, in conjunction with the CIO Council's Y2K Committee and industry, issues an interim rule that (1) establishes a single definition of Y2K compliance in executive branch procurement and (2) generally requires agencies to acquire only Y2K-compliant products and services or those that could be made Y2K compliant.

Appendix I
Timeline of Major Y2K Events



Appendix I
Timeline of Major Y2K Events

November	December	1998 January	February	March	April
	<ul style="list-style-type: none"> OMB accelerates two governmentwide target milestones, moving the date for completion of renovation up 3 months (from December to September 1998) and for implementation up 8 months (from November to March 1999). 	<ul style="list-style-type: none"> President and Vice President discuss the importance of agencies being prepared for the transition to the year 2000 at a Cabinet meeting. 	<ul style="list-style-type: none"> President signs Executive Order 13073 creating the President's Council on Year 2000 Conversion. 	<ul style="list-style-type: none"> OMB requires smaller agencies, for the first time, to report on their Y2K progress. OPM designates the Y2K problem an "unusual circumstance," allowing agencies to temporarily rehire former federal personnel without financial penalty. 	<ul style="list-style-type: none"> Senate passes S. Res. 208, establishing the Special Committee on the Year 2000 Technology Problem to study the impact of Y2K on the executive and judicial branches, state government, and private-sector operations in the United States and abroad. First monthly meeting of the President's Council on Year 2000 Conversion.

Appendix I
Timeline of Major Y2K Events

1998 May	June	July	August	September	October
<ul style="list-style-type: none"> House of Representatives establishes a Year 2000 Task Force, cochaired by the Chairman of the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, and the Chairwoman of the Subcommittee on Technology, Committee on Science. OMB directs tier 1 and tier 2 agencies to report monthly on their Y2K progress. United Nations passes resolution calling on all nations to prepare critical information systems for the century date change. 		<ul style="list-style-type: none"> President's Council, in partnership with National Governors' Association, convenes first Y2K Summit with state and U.S. territory Y2K coordinators. Department of Justice issues a business review letter indicating that information sharing by competitors to try and solve the Y2K problem did not by itself raise an antitrust issue. 	<ul style="list-style-type: none"> GAO issues guidance: <i>Year 2000 Computing Crisis: Business Continuity and Contingency Planning</i> (GAO/AIMD-10.1.19). GAO hosts state/federal auditor conference on Y2K problem. 	<ul style="list-style-type: none"> Vice President and President's Council Chair meet with leaders of federal agencies that according to OMB, were making insufficient progress. 	<ul style="list-style-type: none"> Year 2000 Information and Readiness Disclosure Act (P.L. 105-271) enacted to promote information-sharing among companies testing their Y2K renovations. Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1998 (P.L. 105-277) enacted, appropriating \$2.25 billion for civilian agencies and \$1.1 billion for the Department of Defense for expenses related to Y2K IT conversion. With the help of the Small Business Administration, the Departments of Agriculture and Commerce, and other federal agencies, the President's Council sponsors the first National Y2K Action Week to help businesses, particularly small businesses, make proper Y2K assessments of important systems and take steps to prepare noncompliant systems for the century change. The Chair of the President's Council directs the Council's sector working groups to begin assessing their sectors.

Appendix I
Timeline of Major Y2K Events

November	December	1999 January	February	March	April
<ul style="list-style-type: none"> GAO issues guidance: <i>Year 2000 Computing Crisis: A Testing Guide</i>. (GAO/AIMD-10.1.21). 	<ul style="list-style-type: none"> President's Council helps United Nations organize first meeting of national Y2K coordinators; over 120 countries send representatives. 	<ul style="list-style-type: none"> President's Council issues first quarterly assessment of the Y2K status of the nation's major sectors. President's Council holds its first bimonthly meeting of its Senior Advisors Group, composed of more than 20 Fortune 500 company chief executive officers and heads of major national public-sector organizations. 	<ul style="list-style-type: none"> United Nations establishes the International Y2K Cooperation Center to promote strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on global society and the economy. 	<ul style="list-style-type: none"> President's Council, in partnership with the National Governors' Association, convenes the second Year 2000 Summit with state and U.S. territory Y2K coordinators. OMB's eighth quarterly report provides status of state-administered federal programs for the first time. OMB designates lead agencies for 42 high-impact federal programs (later updated to 43). With the help of the Small Business Administration, the Departments of Agriculture and Commerce, and other federal agencies, the President's Council sponsors the second National Y2K Action Week to help businesses, particularly small businesses, make proper Y2K assessments of important systems and take steps to prepare noncompliant systems for the century change. Federal government goal of completing Y2K implementation by March 1999 is met by 13 of the 24 major departments and agencies. 	<ul style="list-style-type: none"> President's Council issues second quarterly assessment of Y2K status of nation's major sectors.

Appendix I
Timeline of Major Y2K Events

1999 May	June	July	August	September	October
<ul style="list-style-type: none"> OMB requires agencies to submit high-level business continuity and contingency plans. President's Council convenes pharmaceutical roundtable meeting. President's Council convenes food supply roundtable meeting. President's Council launches "Y2K Community Conversations" initiative to promote locally organized town hall meetings to enable citizens to hear from and ask questions of key public and private service providers. 	<ul style="list-style-type: none"> President's Council convenes hospital supply roundtable meeting. President signs an amendment to Executive Order 13073, creating the Information Coordination Center (ICC) to assist the Chair of the President's Council. ICC is charged with making preparations for information-sharing and coordination within the federal government and key components of the public and private sectors, coordinating agency assessments of Y2K emergencies and, if necessary, assisting federal agencies and the Council Chair in reconstitution processes. United Nations holds its second meeting of national Y2K coordinators; over 170 countries send representatives. 	<ul style="list-style-type: none"> President's Council convenes public safety roundtable meeting. Year 2000 Readiness and Responsibility Act (P.L. 106-37) enacted to establish procedures and limitations for civil actions brought for damages relating to the Y2K failure of any device or system. President's Council convenes internet roundtable meeting. 	<ul style="list-style-type: none"> President's Council issues third quarterly assessment of the Y2K status of the nation's major sectors. President's Council convenes chemical roundtable meeting. 	<ul style="list-style-type: none"> President's Council issues <i>100 Days to Y2K: A Resource Guide for Small Organizations</i>. 	<ul style="list-style-type: none"> GAO issues guidance: <i>Year 2000 Computing Challenge: Day One Planning and Operations Guide</i> (GAO/AIMD-10.1.22). President's Council convenes education roundtable meeting. President's Council, in partnership with the National Governors' Association, convenes third Y2K summit with state and U.S. territory coordinators. OMB requires agencies to submit day one plans and revised high-level business continuity and contingency plans.

Appendix I
Timeline of Major Y2K Events

November	December	2000 January	February	March	April
<ul style="list-style-type: none"> President's Council issues <i>Y2K and You</i> informational booklet and personal preparedness checklist. President's Council issues fourth quarterly assessment of Y2K status of the nation's major sectors. Government issues a B+ on final federal report card issued by the House Subcommittee on Government Management, Information and Technology. 	<ul style="list-style-type: none"> OMB announces that 99.9 percent of the federal government's mission-critical systems are Y2K compliant. Beginning December 30, ICC conducts 24-hour monitoring operations for the date rollover period. Staffed primarily with federal agency officials, it obtains and evaluates rollover information from a variety of sources, including federal agencies, states, localities, key private-sector organizations, foreign countries, and the media. 	<ul style="list-style-type: none"> House Y2K Task Force holds final hearing on the results of the century rollover. 	<ul style="list-style-type: none"> Beginning February 28, ICC conducts monitoring operations for leap day rollover. Again staffed primarily with federal agency officials, it obtains and evaluates rollover information from a variety of sources. Senate Special Committee on the Year 2000 Technology Problem issues final report. 	<ul style="list-style-type: none"> GAO convenes Year 2000 Lessons Learned Summit. President's Council issues final report. 	

Appendix II

Participants in GAO's Y2K Lessons Learned Summit

Janet B. Abrams
Executive Director
President's Council on Year 2000 Conversion

Kathleen M. Adams
Vice President and Deputy Director, Health Systems
SRA International, Inc.

David Ames
Deputy Chief Information Officer
Department of State

Senator Robert F. Bennett
Chairman, Special Committee on the Year 2000 Technology Problem
U.S. Senate

Dale Bowen
Director, Online Services
Public Technology, Inc. (PTI)

Dr. Gary Christoph
Chief Information Officer
Health Care Financing Administration
Department of Health and Human Services

Richard A. Clarke
National Coordinator for Security, Infrastructure Protection and
Counterterrorism
National Security Council

Robert Cresanti
Staff Director, Special Committee on the Year 2000 Technology Problem
U.S. Senate

William A. Curtis
Director for IT Investment and Acquisition
Department of Defense/OASD (C3I)

Nancy-Ann DeParle
Administrator
Health Care Financing Administration
Department of Health and Human Services

Appendix II
Participants in GAO's Y2K Lessons Learned
Summit

Thomas V. Fritz
President and Chief Executive Officer
Private Sector Council

Russell George
Staff Director, Subcommittee on Government Management, Information,
and Technology
Committee on Government Reform
House of Representatives

Clay Hollister
Chief Information Officer
Federal Emergency Management Agency

Chairman Stephen Horn
Subcommittee on Government Management, Information and Technology
Committee on Government Reform
House of Representatives

Cathy Hotka
Vice President, Information Technology
National Retail Federation

John Koskinen
Chair
President's Council on Year 2000 Conversion

Charles Madine
Senior Computer Consultant on Y2K
Federal Reserve System

Shirley Malia
Critical Infrastructure Assurance Office
Chair, Chief Information Officers Council's Year 2000 Committee

Chairwoman Constance A. Morella
Subcommittee on Technology
Committee on Science
House of Representatives

Appendix II
Participants in GAO's Y2K Lessons Learned
Summit

Matt Ryan
Senior Policy Adviser
Subcommittee on Government Management, Information and Technology
Committee on Government Reform
House of Representatives

Ed Springer
Senior Policy Analyst
Office of Management and Budget

Cynthia M. Warner
Director, Strategic IT Issues Division
General Services Administration

Benjamin H. Wu
Professional Staff Member
Subcommittee on Technology
Committee on Science
House of Representatives

GAO Reports and Testimony Statements Addressing the Year 2000 Computing Challenge

Social Security Administration: Year 2000 Readiness Efforts Helped Ensure Century Rollover and Leap Year Success(GAO/AIMD-00-125, April 19, 2000)

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

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software(GAO/AIMD-00-55, December 23, 1999)

Year 2000: Insurance Regulators Have Accelerated Oversight, but Some Gaps Remain (GAO/GGD-00-42, December 20, 1999)

Year 2000 Computing Challenge: Readiness of FBI's National Instant Criminal Background Check System Can Be Improved(GAO/AIMD/GGD-00-49, December 16, 1999)

Defense Computers: U.S. Space Command's Management of Its Year 2000 Operational Testing (GAO/AIMD-00-30, November 15, 1999)

Defense Computers: U.S. Transportation Command's Management of Y2K Operational Testing (GAO/AIMD-00-21, November 15, 1999)

Year 2000 Computing Challenge: Noteworthy Improvements in Readiness But Vulnerabilities Remain (GAO/T-AIMD-00-37, November 4, 1999)

Year 2000 Computing Challenge: Federal Business Continuity and Contingency Plans and Day One Strategies(GAO/T-AIMD-00-40, October 29, 1999)

Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls(GAO/AIMD-00-24, October 29, 1999)

Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs (GAO/T-AIMD-00-39, October 28, 1999)

Reported Y2K Readiness of State Employment Security Agencies' Unemployment Insurance Benefits and Tax Systems(GAO/AIMD-00-28R, October 28, 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Challenge: Nuclear Power Industry Reported Nearly Ready; More Reduction Measures Can Be Taken (GAO/T-AIMD-00-27, October 26, 1999)

Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans (GAO/AIMD-00-11, October 22, 1999)

Year 2000 Computing Challenge: Compliance Status Information on Biomedical Equipment (GAO/T-AIMD-00-26, October 21, 1999)

Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning (GAO/T-AIMD-00-25, October 21, 1999)

Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management (GAO/AIMD-00-12, October 18, 1999)

Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning (GAO/AIMD-00-8, October 14, 1999)

Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs (GAO/T-AIMD-00-9, October 6, 1999)

Reported Medicaid Year 2000 Readiness (GAO/AIMD-00-22R, October 5, 1999)

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

Y2K Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, October 1999)

Year 2000 Computing Crisis: Readiness of the Telecommunications Industry (GAO/AIMD-99-293, September 30, 1999)

Year 2000 Computing Challenge: Readiness of USDA High-Impact Programs Improving, But More Action Is Needed (GAO/AIMD-99-284, September 30, 1999)

Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues (GAO/T-AIMD-99-299, September 27, 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Challenge: Status of the District of Columbia's Efforts to Renovate Systems and Develop Contingency and Continuity Plans (GAO/T-AIMD-99-297, September 24, 1999)

Year 2000 Computing Challenge: The District of Columbia Cannot Reliably Track Y2K Costs (GAO/T-AIMD-99-298, September 24, 1999)

Reported Year 2000 (Y2K) Readiness Status of 25 Large School Districts (GAO/AIMD-99-296R, September 21, 1999)

IRS' Year 2000 Efforts: Actions Are Under Way to Help Ensure That Contingency Plans Are Complete and Consistent (GAO/GGD-99-176, September 14, 1999)

Year 2000 Computing Challenge: FAA Continues to Make Important Strides, But Vulnerabilities Remain (GAO/T-AIMD-99-285, September 9, 1999)

Year 2000 Computing Challenge: SBA Needs to Strengthen Systems Testing to Ensure Readiness (GAO/AIMD-99-265, August 27, 1999)

Nuclear Weapons: Year 2000 Status of the Nation's Nuclear Weapons Stockpile (GAO/RCED-99-272R, August 20, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Essential Actions Remain to Ensure Delivery of Critical Services (GAO/T-AIMD-99-268, August 17, 1999)

Year 2000 Computing Challenge: Important Progress Made, But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-267, August 14, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-266, August 13, 1999)

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems (GAO/AIMD-99-218, August 5, 1999)

Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Status of Medicare Providers Unknown
(GAO/AIMD-99-243, July 28, 1999)

Reported Y2K status of the 21 Largest U.S. Cities(GAO/AIMD-99-246R,
July 15, 1999)

*Year 2000 Computing Challenge: Federal Efforts to Ensure Continued
Delivery of Key State-Administered Benefits*(GAO/T-AIMD-99-241, July 15,
1999)

*Emergency and State and Local Law Enforcement Systems: Committee
Questions Concerning Year 2000 Challenges*(GAO/AIMD-99-247R, July 14,
1999)

*Year 2000 Computing Challenge: Important Progress Made, Yet Much Work
Remains to Avoid Disruption of Critical Services* (GAO/T-AIMD-99-234,
July 9, 1999)

*Year 2000 Computing Challenge: Readiness Improving Yet Avoiding
Disruption of Critical Services Will Require Additional Work*(GAO/T-AIMD-
99-233, July 8, 1999)

*Year 2000 Computing Challenge: Readiness Improving But Much Work
Remains to Avoid Disruption of Critical Services* (GAO/T-AIMD-99-232,
July 7, 1999)

*Defense Computers: Management Controls Are Critical to Effective Year
2000 Testing* (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs Is Making Good Progress (GAO/T-
AIMD-99-225, June 29, 1999)

*Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States'
Achieving Compliance* (GAO/T-AIMD/GGD-99-221, June 23, 1999)

*Year 2000 Computing Challenge: Estimated Costs, Planned Uses of
Emergency Funding, and Future Implications*(GAO/T-AIMD-99-214,
June 22, 1999)

*GSA's Effort to Develop Year 2000 Business Continuity and Contingency
Plans for Telecommunications Systems* (GAO/AIMD-99-201R, June 16,
1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services(GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions(GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999)

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems (GAO/T-AIMD-99-8, October 8, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998)

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 28, 1998)

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations at Risk (GAO/AIMD-98-150, June 30, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

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)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach (GAO/T-AIMD-97-173, September 25, 1997)

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

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

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

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

Appendix III
GAO Reports and Testimony Statements
Addressing the Year 2000 Computing
Challenge

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses(GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization(GAO/T-AIMD-97-91, May 16, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now(GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology(GAO/HR-97-9, February 1997)

Appendix IV

Comments From the Office of Management and Budget

DEPUTY DIRECTOR
FOR MANAGEMENTEXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 5, 2000

Mr. Jeffery C. Steinhoff
Assistant Comptroller General
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Steinhoff:

This is in response to your letter of August 17, 2000 which forwarded a draft report entitled, "Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges" (GAO/AIMD-00-290). Having led the Executive Branch's effort to address the Y2K problem in Federal systems and programs, we read the draft report with great interest. There is no question that successfully addressing the year 2000 computing challenge was a major test of the Federal government and indeed the nation. It was one of the most complex management challenges the Federal government has ever faced, and it potentially had enormous implications for our economy, and for all organizations large and small.

We agree with the draft report that leadership and coordination and communication were key elements in the success of the Y2K effort. This is particularly true within the Federal government. Certainly it was essential to the success of the Y2K effort that the Executive branch worked closely with the Congress and your Office. This was also true in establishing the measures of progress we used in tracking our efforts. It was also critical that we coordinated our efforts with State, local and tribal governments as well as the private sector and internationally. As the enormity of the Y2K challenge became apparent, the President created his project team, the Year 2000 Conversion Council, to address it. As the draft report describes, the Council communicated and coordinated with all sectors of the economy that could be affected by the problem, effectively motivating and assisting their efforts. We also agree that assuring human capital and adequate funding were essential to the success of the effort.

We are pleased that the GAO found benefits from the Y2K effort other than the primary one of assuring a smooth and uneventful rolldate, and agree that agencies should take maximum advantage of such benefits. We note, however, that the effort was undertaken with the single purpose of fixing the Y2K problem regardless of any such secondary benefits.

We also agree that the momentum from the Y2K success can be helpful in addressing the three other management challenges that are described in the report. In applying lessons learned from the Y2K effort, however, we should recognize what it was – the Y2K effort was a project focused on fixing a finite problem which had a fixed, unmovable deadline. It was a vast management

Appendix IV
Comments From the Office of Management
and Budget

challenge, but it did not involve difficult technical challenges. Over the course of the effort, our understanding of how the problem might manifest itself grew, but the nature of the technical problem did not change. In this sense the problem was benign and thus much simpler than other key IT challenges, such as the problem of assuring effective computer security which involves a rapidly changing technical threat. Similarly, in the Y2K project there was no need to invest in research and development for the longer term. However, because of the changing technical threat, critical infrastructure protection and computer security need such investment, and we proposed \$606 million in the President's FY 2001 budget for it. Thus the approach that worked for the Y2K problem may or may not be the most effective one for addressing those other challenges. Rather, we must address each of the three management challenges in its own context.

We also note that while the report identifies several key lessons to be learned from the Y2K effort, there were several other lessons that should be noted:

First and foremost is the lesson that we have many dedicated employees and contractors who were willing to go beyond their normal duties and responsibilities to tackle the problem. While we at OMB contributed to the success of the effort, we did not change one line of code or fix one system. The heroes of the Y2K effort are the technicians who worked long and hard implementing fixes to and testing the thousands of systems that we depend upon. Our role, and that of agency headquarters staff was to provide leadership and assistance to those workers -- but credit for the success of efforts to fix the problem in Federal systems belongs to them.

A second lesson is that there is a robust information technology marketplace that, given a problem will move rapidly to address it. Early in the effort, most thought that there would not be enough technicians available to fix all of the lines of code in all of the systems that needed to be fixed. However, once the problem to be solved was recognized, products began to appear in the marketplace to partially automate its solution. Ultimately those products were improved and they improved worker productivity from hundreds of lines of code a day to the potential to do more than a million a day. The result was that rather than having a shortage of technicians to fix code, there was an abundance. I might add that such tools were invaluable to those who started late on the problem, such as those overseas, in being able to fix the problem on time.

Another lesson learned, which is briefly alluded to in the report, is the value of openness. The year 2000 problem affected all Federal agencies as well as all States and most private sector organizations. Sharing best practices in managing the problem as well as technical information was quite helpful to all involved. But beyond that, the President's Y2K Council openly shared all information it had concerning the problem and progress in addressing it with the public. Armed with that information, the public did not over-react in preparing for the rollover.

Finally, the report suggests that the Congress consider the establishment of a Federal CIO to address the other IT management challenges mentioned in the report. As the draft report notes, OMB has not supported creating a new office for this purpose. The Administration believes that, as Congress recognized in the Clinger-Cohen Act, the requisite authorities such an office should have are already vested in the Deputy Director for Management in OMB. The success of the Y2K does not suggest otherwise. The President's Y2K Council was focused on a single issue for a

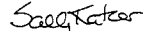
Appendix IV
Comments From the Office of Management
and Budget

finite period of time, and the Chair of the Council was not a CIO. He was selected largely for his managerial, not his technology, expertise, having just stepped down as OMB's Deputy Director for Management.

I should also note that, while the Council had oversight of efforts to address the totality of the Y2K problem, OMB was in charge of efforts to address the problem in Federal programs and systems. We did that by creating a team of several individuals who worked for the Deputy Director for Management. Those individuals are now working on other activities, including the management challenges identified in the draft report, and as the Deputy Director for Management. I remain responsible to the Director for leadership in Federal information resources and information technology management.

Thank you for the opportunity to comment on the draft report. I look forward to our continued close working relationship on this and other matters.

Sincerely,



Sally Katzen
Deputy Director for Management

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. 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

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

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
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.

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, or 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)

Mr. HORN. We thank you very much for the usual fine analysis by the General Accounting Office.

We now move to Mr. Jim Flyzik, the Deputy Assistant Secretary, Information Systems and the Chief Information Officer for the Department of the Treasury, and he's here in that role as well as being vice chairman, Chief Information Officers Council. And we are particularly interested through you as to the views the Chief Information Officers have on these matters.

Mr. Flyzik.

STATEMENT OF JIM FLYZIK, DEPUTY ASSISTANT SECRETARY, INFORMATION SYSTEMS, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF THE TREASURY, VICE CHAIRMAN, CHIEF INFORMATION OFFICERS COUNCIL

Mr. FLYZIK. Thank you, Mr. Chairman, Mr. Turner, Mr. Davis, and members of the subcommittee. I appreciate the opportunity to appear today to discuss the concept of a Federal Chief Information Officer. I would like to first thank the chairman and the other members of the subcommittee for your continued support and interest in the improvement of information technology performance and accountability in the Federal Government.

I have served as the vice chair of the Federal CIO Council since 1998, where I play a key role in the direction of information technology for the Federal Government. In performing my jobs, I have witnessed the growth of online services changing the way customers expect to interact with their government. Citizens now want to use technology to access the government and its services at a time and a location that is convenient to them. It is no longer acceptable to have a 9 by 5 government. Kiosks, the Internet and voice technologies are just a few examples of the many technologies that exist to provide a fully interactive government to our citizens based on their terms.

Due to factors including the Clinger-Cohen legislation, the work of the Federal CIO Council, the year 2000 success and the growth of the Internet and e-commerce, the role of the Federal CIO is progressing into a peer with senior management. I appeared before this subcommittee in March to discuss the differences in the role of a CIO in the public and private sectors. Attention is now turning to the future potential and growth of Federal CIOs. One option under discussion is creation of a new Federal CIO within the Executive Office of the President.

In regard to this question, the subcommittee presented me with six questions which I would like to briefly address. Should there be a Federal CIO and, if so, how should it assist the Federal Government in managing information technology? The attention and debate now surrounding this question is quite timely. As we progress to a new administration we must envision the government in an interconnected digital world. My opinion of whether a new position of Federal CIO is a good idea would depend on how the position would be implemented and empowered. A major constraint to the pace of IT advancement in government has been the skirmishes over centralization versus decentralization, not lack of capability.

As vice chair of the CIO Council I believe that many government programs that share common elements or information could be

vastly improved with stronger authority to enforce interagency and intergovernmental cooperation. We need to tear down stovepipes and obsolete hierarchical structures. The Internet knows no such structures or boundaries.

Mr. HORN. Could I just interject for a minute because I've heard the term yesterday and today, and would you explain to everybody what a stovepipe approach is?

Mr. FLYZIK. Yes, sir. In traditional ways that stoves worked in homes in the past, you would have various pipes going out that all were independent of one another with no coordination. So when we talk about stovepipes we view our agencies working independently without cooperating or toward one common goal.

Mr. HORN. Well, now that we have a definition every one that comes up from the administration will have a little asterisk put by their name as the Flyzik view of stovepipes. It will be put in all hearings.

Mr. FLYZIK. Thank you so much, sir. It's nice to know I have a legacy here.

Mr. HORN. We try to provide those little services.

Mr. FLYZIK. The oversight could continue to be in the form of the OMB Deputy Director for Management or it could be another option like a new Federal CIO or a more empowered CIO Council. Any new leadership position in this area should have authority to work through the Director of OMB to control IT resources, IT budgets and spending. The centralized leadership can assist the government in managing its use of information technology and, like the Deputy Director of Management does today, assist the administration efforts to advise the President on matters relating to IT, build a vision for IT in the Federal sector, create opportunities and partnerships with the academic and private sector, set the direction for critical IT areas to cross agency boundaries such as interactive government and security, privacy and critical infrastructure protection and, importantly, enforce a Federal enterprize architecture and, most importantly, see government programs functionally from the point of view of the customer, not any specific agency. We can and should build on this framework.

Where should the position be located? As the Deputy Director of Management today, any enhanced central authority over interagency IT initiatives needs to be located within the Executive Office of the President. Progress and success will require buy-in from agency heads; therefore, the function needs to be performed at a level that can deal with cabinet officers.

How should it be empowered? Stronger empowerment requires actual authority in a budget to initiate and oversee the direction and funding of IT initiatives that affect more than one agency. A new staff position with primary duties to chair a council or review presentations or present recommendations would be viewed as just another bureaucratic hurdle and would be counterproductive. It is essential that any enhanced authority continue to be integrally linked with OMB's budget function to develop a process for evaluating the performance of capital investments for IT across government. It is also essential that any centralized position have authority to develop a process for funding interagency initiatives.

Improved funding and management of multiagency IT initiatives can enhance the government's ability to address common IT challenges and solutions. Technology allows us to provide government to its customers across functional areas. The funding mechanisms should be developed to support this approach. In addition, funds for interagency IT should be solidified and made sufficient to support the level of need for interagency work.

How should a Federal CIO's relationship with agency CIOs in the Federal CIO Council be defined? A digital economy drives new expectations of government. It would make sense that it would drive a new structure too. Ontario, Canada provides an example of a structure based on functional areas of government rather than agency structures. Before Ontario changed its structure the 17 different ministries had 17 different CIOs reporting to the deputy minister and cabinet office. Now there is a single authority that reports to the cabinet office in charge of information technology and is held accountable for IT in Ontario.

What are more interesting are clusters of CIOs created around communities of service. The CIOs of these clusters report to the Ontario CIO. Leadership of Federal IT can operate in a similar fashion. The Federal CIO Council is already in place and could present the clusters of CIOs. I provide a chart of the Ontario organization as an example of a structure evolving with technology.

How should a Federal CIO address issues such as electronic government information and insurance? Any expanded central authority should build on the structure currently in place, the Federal CIO Council. The Council is effective at establishing committees to bring subject matter experts out to address the issues and are in the forefront of IT in government-electronic government. Enterprise interpretability; capital planning; security, privacy and critical infrastructure protection; and Federal IT work force are some examples. The Council has developed a strategic plan with specific goals and initiatives for each committee. Greater authority could give the Federal CIO Council the responsibility and resources it requires to work with agencies states, academia and the private sector.

Finally, question 6, what are the other key issues the Federal CIO should consider? Any action to strengthen central authority for governmentwide IT strategy should continue to work closely with the Federal CIO Council to develop strategies. Issues we have identified are: Connecting citizens to product services and information of their government; putting in place interoperable and governmentwide IT initiatives; providing a secure and reliable information infrastructure that the customer can access and trust; acquiring IT skills and resources to meet mission objectives; collaborating between the public and private sectors to achieve better government; fostering investment management policies, practices and tools that enable improved delivery of government programs and services.

I find that the two proposed pieces of legislation are, each in different ways, interesting starts in improving the coordination and effectiveness of IT efforts. It is refreshing that reducing the burden of information collection from the citizen is emphasized.

We look forward to working with the Congress on addressing these and other issues. I would like to thank the subcommittee for

the support it has given to the work of the Federal CIO Council. Without your support we would not have been able to achieve the national success we have enjoyed with Y2K, the Internet and e-government. I would like to thank the members of the subcommittee for the opportunity to present this morning.

Mr. Chairman, this concludes my formal remarks. I look forward to answering questions.

[The prepared statement of Mr. Flyzik follows:]

TEXT AS PREPARED FOR DELIVERY

September 12, 2000

**TREASURY DEPUTY ASSISTANT SECRETARY (INFORMATION SYSTEMS)
AND CHIEF INFORMATION OFFICER (CIO) TESTIMONY BEFORE THE
HOUSE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY**

Mr. Chairman and members of the Subcommittee, I appreciate the opportunity to appear today to discuss the concept of the Federal Chief Information Officer as proposed in the Federal Information Policy Act and the Chief Information Officer of the United States Act. I would like to thank the Chairman and the other members of the Subcommittee for your continued support and interest in the improvement of information technology performance and accountability in the Federal Government.

I serve as the Deputy Assistant Secretary for Information Systems and Chief Information Officer for the Treasury Department. In this role, I provide strategic direction, oversight and management of all information technology programs within the Treasury Department and its fourteen Bureaus. Since February of 1998, I have served as the Vice Chair of the

Federal CIO Council where I play a key role in the direction of information technology for the Federal Government. I also served as Chairman of the Government Information Technology Services Board (GITSB). In performing these jobs, I have witnessed the growth of online services changing the way customers expect to interact with their government. Citizens now want to use technology to access the government and its services at a time and a location that is convenient to them. It is no longer acceptable to have a "9 by 5" government. Kiosks, the Internet, and voice technologies are just a few examples of the many technologies that exist to provide a fully interactive government to our citizens based on their terms.

Due to factors including the Clinger-Cohen legislation, the work of the Federal CIO Council, the Year 2000 success, and the growth of the Internet and E-Commerce, the role of the Federal CIO is progressing into a peer with senior management. I appeared before this subcommittee in March to discuss the differences in the role of a CIO in the public and private sectors. Attention is now turning to the future growth and potential of Federal CIOs. One option under discussion is the creation of a new Federal CIO within the Executive Office of the President.

In regard to this issue, the subcommittee presented me with six questions that I would now like to address:

Question 1.) Should there be a Federal CIO, and if so, how should it assist the Federal Government in managing its use of information technology?

Answer: The attention and debate now surrounding this question is timely. As we progress to a new Administration, we must envision a government in an interconnected digital world. My opinion of the whether a new position of federal CIO is a good idea would depend on how the position would be implemented and empowered. A major constraint to the pace of information technology (IT) advancement in government has been the skirmishes over centralization versus decentralization, not lack of capability.

This Administration has been very active in establishing the foundation for IT leadership, through the enactment and implementation of Clinger Cohen, the creation of the CIO Council, the success of Y2K, and now increased attention to electronic government and computer security. Indeed, in 1996, Congress and the President in the Clinger-Cohen Act ushered in a new era -- a move toward agency empowerment and accountability for IT results, along with additional oversight and accountability from the Deputy Director of Management. Clinger-Cohen has been in effect for only four years. Much progress has already been achieved. OMB has issued the Raines Rules, and has institutionalized the budget review of IT acquisitions through A-11 and A-130. This progress was made at the same time that OMB and the agencies had to divert their attentions and mount an all-consuming effort to overcome the Y2K problem. Now that we have moved past Y2K, we can turn our attention 100% to implementing Clinger-Cohen and reaping the benefits of our past efforts and our ongoing and future initiatives.

As Vice-Chair of the CIO Council, I believe that many government programs that share common elements or information could be vastly improved with stronger authority to

enforce interagency and intergovernmental cooperation. We need to tear down stovepipes and obsolete hierarchical structures. The Internet knows no such structures or boundaries. The oversight could continue to be in the form of the OMB Deputy Director for Management, or could be in another option like a new federal CIO or a more empowered CIO Council. Any new leadership position in this area should have authority to work through the Director of OMB to control IT resources, IT budgets, and spending. The centralized leadership can assist the government in managing its use of information technology and, like the Deputy Director of Management does today, assist the Administration efforts to:

- advise the President on matters relating to IT;
- build a vision for IT in the federal sector;
- create opportunities and partnerships with the academic and private sector communities;
- set the direction for critical IT areas that cross agency boundaries such as interactive government and security, privacy and critical infrastructure protection;
- enforce a federal enterprise architecture; and

most importantly, see government programs functionally from the point-of-view of the customer, not any specific agency. We can and should build on this framework.

Question 2.) Where should such a position be located within the Federal Government?

Answer: As is the Deputy Director of Management today, any enhanced central authority over interagency IT initiatives needs to be located within the Executive Office of the

President. Information technology has become a part of every dialogue concerning the business decisions and the security of our government. The effective management of IT across multiple stakeholders requires a commitment to view IT from an enterprise perspective. Progress and success will require buy in from Agency Heads. Therefore, the function needs to be performed at a level that can deal with cabinet officers.

Question 3.) How should this position be empowered?

Answer: Stronger empowerment for leadership on interagency IT initiatives requires actual authority and a budget to initiate and oversee the direction and funding of IT initiatives that affect more than one federal agency. A new staff position with primary duties to chair a council, review presentations of initiatives, and present recommendations would be viewed as just another bureaucratic hurdle and would be counterproductive.

It is essential that any enhanced authority continue to be integrally linked with OMB's budget function to develop a process for evaluating the performance of capital investments for information technology across government. It is also essential that any centralized position have authority to develop a process for the funding of interagency initiatives. Improved funding and management of multi-agency IT initiatives can enhance the government's ability to address common IT challenges and solutions. Technology allows us to provide government to its customers across functional areas. The funding mechanisms should be developed to support this approach. In addition,

funds for interagency IT should be solidified and made sufficient to support the level of need for interagency work.

Question 4.) How should a Federal CIO's relationship with agency CIOs and the Federal CIO Council be defined?

Answer: A digital economy drives new expectations of government. It would make sense that it would drive a new structure too. Ontario, Canada provides an example of a structure based on functional areas of government rather than agency structures. Before Ontario changed its structure, the 17 different ministries had 17 different CIOs reporting to the Deputy Minister and the Cabinet Office. Now there is a single authority that reports to the Cabinet Office in charge of information technology and is held accountable for IT in Ontario. What are more interesting are the clusters of CIO's created around communities of service. The CIO's of these clusters report to the Ontario CIO.

Leadership of Federal IT could operate in a similar fashion. The Federal CIO Council is already in place and could represent the clusters of CIOs. I have provided charts of the Ontario organization as an example of a structure evolving with technology.

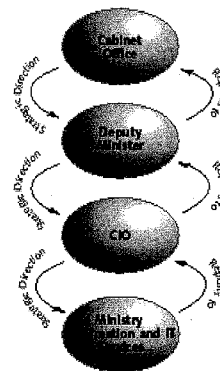


Chief Information Officer of Ontario

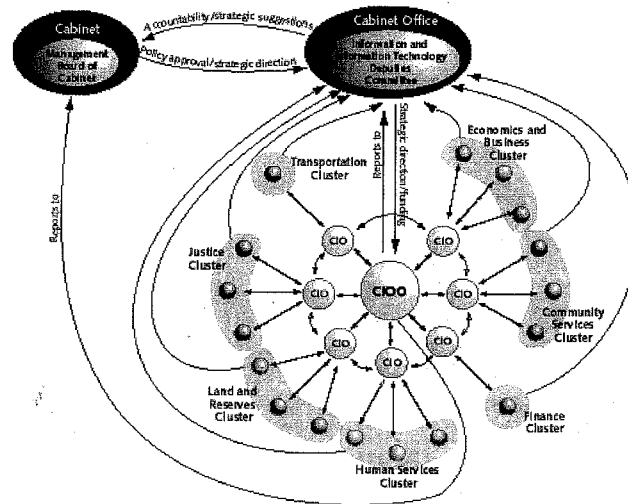
horizontal integration of the structure and management of IT systems, policies and people across government.

Before:

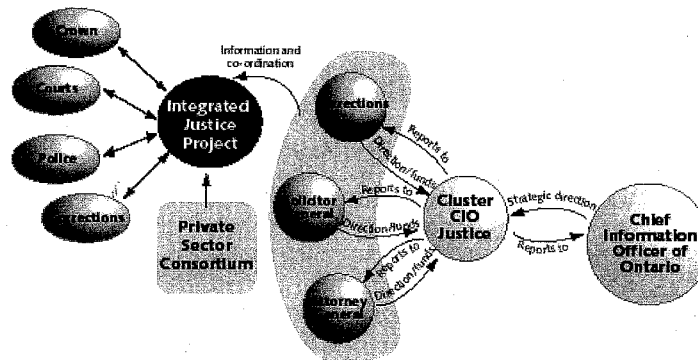
Structure for each of 17 ministries before the IT strategy



After: Case: Province of Ontario



Justice Cluster CIO



Question 5.) How should a Federal CIO address key issues such as electronic government and information assurance?

Answer: As the Deputy Director of Management does today, any expanded central authority for interagency IT initiatives should build on the structure currently in place - the Federal CIO Council. The Federal CIO Council is effective at establishing committees to bring subject matter experts out to address the issues that are at the forefront of IT in government- electronic government; enterprise interoperability; capital planning; security, privacy and critical infrastructure protection; and federal IT workforce are some examples. The Council has developed a strategic plan with specific goals and initiatives for each committee. Greater authority could give the Federal CIO Council the responsibility and resources it requires to work with agencies, states, academia and the private sector to bring interactive government to its citizens.

Question 6.) What are the other key issues a Federal CIO should consider in developing short-and long-term information technology strategies for the Federal Government?

Answer: Any action to strengthen central authority for government-wide IT strategies should continue to work closely with the Federal CIO Council to develop IT strategies. Issues the Council has identified are:

1. Connecting citizens to the products, services, and information of their government.

2. Putting in place interoperable and innovative government-wide IT initiatives.
3. Providing a secure and reliable information infrastructure that the customer can access and trust.
4. Acquiring IT skills and resources to meet mission objectives.
5. Collaborating between the public and private sectors to achieve better government.
6. Fostering investment management policies, practices and tools that enable improved delivery of government programs and services.

I find that the two proposed pieces of legislation - the Federal Information Policy Act and the Chief Information Officer of the United States Act, are, each in different ways, interesting starts at improving the coordination and effectiveness of IT efforts. It is refreshing that reducing the burden of information collection from the citizen is emphasized. However, HR 5024 does contain very prescriptive budget and process requirements. We look forward to working with the Congress on addressing these and other issues.

I would like to thank the subcommittee for the support it has given to the work of the Federal CIO Council. Without your support we would not have been able to achieve the National success we have enjoyed with Y2K, the Internet and E-Government. I would like to thank the members of the Subcommittee for the opportunity to present this morning. Mr. Chairman, this concludes my formal remarks and I would be happy to respond to any questions.

Mr. HORN. Well, thank you very much. We appreciate that summary.

Otto Doll is the Commissioner of the Bureau of Information and Technology for the State of South Dakota and president of the National Association of State Information Resources Executives. I'm particularly indebted to you for those nice charts you put with your testimony. It's very helpful to see what the Governors are doing around the country.

So Mr. Doll.

STATEMENT OF OTTO DOLL, COMMISSIONER, BUREAU OF INFORMATION & TECHNOLOGY, STATE OF SOUTH DAKOTA, PRESIDENT, NATIONAL ASSOCIATION OF STATE INFORMATION RESOURCES EXECUTIVES

Mr. DOLL. Thank you, Mr. Chairman, Mr. Turner, Mr. Davis, and members, subcommittee members. Recent congressional bills such as H.R. 4670 and H.R. 5024 offer tremendous opportunities for the Federal Government to take full advantage of the Internet revolution and all it has to offer for digital government. The States, as laboratories of democracy, offer many examples of how enterprise-wide Chief Information Officers add real value to government's use of information technology. Furthermore, the recent year 2000 compliance effort has allowed all CIOs, whether they be local, Federal, State, private or public sector, to completely inventory the IT resources at their disposal. For the first time we have been able to establish lines of communication and cooperation among IT units through our enterprises.

While it is difficult to derive a single organizational model from the 50 States, some clear trends are apparent, and both of the bills cited earlier put the Federal Government firmly on the same path.

Generally with the title CIO comes advisory responsibility for enterprise-wide IT policy, not just management. Many, if not all, CIOs report to their Governors, State chief executives in some formal or informal capacity. CIOs can be called upon to advise the Governor on IT matters, deliver agency IT budgets, draft proposal legislation, testify before legislative committees on IT investment options and results and oversee statewide procurement, project management, risk management and strategic planning. While many State CIOs report solely to their Governors on technology issues, some are also responsible to cabinet level officials such as the secretary of administration, commerce, or revenue.

According to a survey conducted by NASIRE in February and staff research, 23 States have a CIO in place who reports directly to the Governor; only 8 States reported such an arrangement in a 1998 survey; 24 State CIOs operate within some other arrangement, usually reporting to a cabinet officer. However, that does not mean those CIOs never interact with their Governors. Some State CIOs work in conjunction with an advisory board or commission and many serve as chair of a council of agency level CIOs. The remaining three States are currently moving toward a CIO arrangement.

A roundtable of State CIOs held at NASIRE's 2000 midyear conference discussed key aspects of real CIO authority. The clear consensus was that some form of access to the Governor is crucial to

the CIO's success. Without that access the CIO cannot win the sponsorship that is necessary to implement innovative application of technology, break down the silos of government and manage the expectations of internal and external constituents who are often intimidated by or over expectant of the impact of IT on government.

The recent Federal experiences with John Koskinen, who served as the Y2K czar, shows how a CIO level official serving as an extension of the chief executive can bring together diverse public and private interests to tackle the huge IT project.

We have also seen how the President's keen interest in the development of the FirstGov.gov portal has reinvigorated a project that had previously floundered without centralized high level leadership. The Oval Office and Congress will need an ongoing, accountable IT visionary for future efforts.

The necessity of the CIO has been recognized by a number of organizations, including the National Electronic Commerce Coordinating Council, which declared: "regardless of the structure, the most critical factor for success in implementing electronic government is a clear direction communicated with both authority and responsibility. Responsibility for implementation should rest with an empowered leader, such as the CIO."

NEC3 is a coalition among NASIRE, the National Association of Secretaries of State, the National Association of State Procurement Officials, and the National Association of State Auditors, Comptrollers and Treasurers.

Separating technology from government programs is impossible today. State CIOs are responsible for putting their executives visions and goals for IT into action. The Harvard Policy Group on Network-Enabled Services and Government, which included CIOs from all levels of government, echoes that sentiment. They define CIO not solely as a manager of technology but as a manager of technology in support of organizational strategy and change management. The same sentiment emerges from the private sector as well.

Janet Caldwell of IBM's Institute for Electronic Government states: "our early studies with the Kennedy School of Government revealed that a center of gravity for technology policy and strategy is a fundamental critical success factor for governments to move forward aggressively. That can come in the form of a Chief Information Officer or a technology and policy advisor to the chief executive."

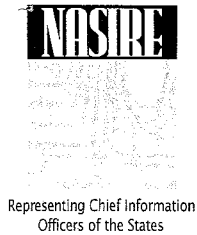
As the center of gravity for IT policy, the CIO needs to inspire leaders, including elected and appointed officials as well as front line managers and staff that dedicate political capital and other resources to the agenda. One powerful dynamic of IT is that it can enable and integrate all government services and initiatives—education, criminal justice, economic development, etc.

A CIO is necessary to convene key information stakeholders, develop adaptive architectures that are conducive to sharing, and access the incumbent risks of exposing information online. Then the CIO is needed to moderate the changing interest of the diverse stakeholders, enforce standards for sharing, and implement the critical security technologies and processes that can ensure privacy. Only then will government enjoy the full benefits of integration.

Globally, a number of other nations are taking aggressive approaches to digital government, including the Special Administrative Region of Hong Kong, Singapore, Australia, Canada, United Kingdom and the European Union. Australia represents a major effort to have all that nation's services well enabled by 2001. Australia, Hong Kong and Singapore have also signed memoranda of understanding to facilitate cross national e-commerce, underscoring the important role a national digital government can play in facilitating economic growth.

In conclusion, let me say that my goals for today have been to reinforce my testimony before this committee from last March. Support for the role of the CIO comes from many quarters. Furthermore, empowered CIOs such as those in Kentucky and Indianapolis and elsewhere can achieve much. NASIRE encourages the Federal Government to establish an Executive Office of the CIO. However, we caution that the role CIO cannot be defined with one act. The work of the CIO will not end after one project. In our estimation, the future success of any government in the new economy depends on not only establishing an office of the CIO, but also in constantly evolving the role of CIO as technologies change and new opportunities emerge. Only then will the full fruition of digital government be within our reach.

[The prepared statement of Mr. Doll follows:]



**STATEMENT OF OTTO DOLL
PRESIDENT
NASIRE – REPRESENTING CIOs OF THE STATES**

**UNITED STATES CONGRESS -
SUBCOMMITTEE ON GOVERNMENT
MANAGEMENT, INFORMATION, AND
TECHNOLOGY**

SEPTEMBER 12, 2000

I. NASIRE Testimony

II. Attachments

- A.** Text from State CIO Roundtable Discussion -
NASIRE's 2000 Mid-Year (Spring) Conference
- B.** Text of House Bill 789 – state of Kentucky 1998 General Session
- C.** Map Identifying State CIO Authority

**STATEMENT OF OTTO DOLL
PRESIDENT, NASIRE – REPRESENTING
CHIEF INFORMATION OFFICERS OF THE STATES
BEFORE THE
UNITED STATES CONGRESS -
SUBCOMMITTEE ON GOVERNMENT
MANAGEMENT, INFORMATION, AND TECHNOLOGY**

SEPTEMBER 12, 2000

Recent Congressional bills, such as H.R. 4670 and H.R. 5024, offer tremendous opportunities for the Federal government to take full advantage of the Internet Revolution and all it has to offer for digital government. The states, as laboratories of democracy, offer many examples of how enterprise-wide chief information officers (CIOs) add real value to government use of information technology (IT). Furthermore, the recent Year 2000 compliance effort has allowed all CIOs, whether they be local, state, federal, or private- or public-sector, to completely inventory the IT resources at their disposal.¹ For the first time, we have also been able to establish lines of communication and cooperation among IT units throughout our enterprises.

While it is difficult to derive a single organizational “model” from the 50 states, some clear trends are apparent, and both of the bills cited earlier put the Federal government firmly on the same path. Generally, with the title “CIO” comes advisory responsibility for enterprise-wide IT policy, not just management. Many, if not all, CIOs report to their governors, the state’s chief executives in some formal or informal capacity. CIOs can be called upon to advise the governor on IT matters, deliver agency IT budgets, draft proposed legislation, testify before state legislative committees on IT investment options and results, and oversee statewide procurement, project management, risk management, and strategic planning. While many state CIOs report solely to their governors on technology issues, some are also responsible to cabinet-level officials, such as the secretary of administration, commerce, or revenue.

According to a survey conducted by NASIRE in February and staff research, 23 states have a CIO in place who reports directly to the governor. (Only eight states reported such an arrangement in a 1998 survey.) Twenty-four state CIOs operate within some other arrangement, usually reporting to a cabinet-level officer. However, that does not mean those CIOs never interact with their governors. Some state CIOs work in conjunction with an advisory board or commission and many of them serve as chair of a council of agency-level CIOs. The remaining three states are currently moving toward a CIO arrangement.

A roundtable of state CIOs held at NASIRE’s 2000 Mid-Year Conference discussed key aspects of “real CIO authority.” The clear consensus was that some form of access to the governor is crucial to the CIO’s success. Without that access, the CIO cannot win the sponsorship that is necessary to implement innovative application of technology, break down the silos of government, and manage the expectations of internal and external constituents, who are often intimidated by, or over-expectant of, the impact of IT on government.

¹ Intergovernmental Advisory Board (IAB), “The Many Silver Linings of The Year 2000 Challenges,” January 2000, <<http://policyworks.gov/intergov/SilverL-Cover.htm>> (31 August 2000), 5.

The recent Federal experience with John Koskinen, who served as the “Y2K Czar,” shows how a CIO-level official, serving as an extension of the Chief Executive, can bring together diverse public and private interests to tackle a huge IT project. We have also seen how the President’s keen interest in the development of the Firstgov.gov portal has reinvigorated a project that had previously floundered without centralized, high-level leadership.² The Oval Office and Congress will need an ongoing, accountable IT visionary for future efforts.

The necessity of the CIO has been recognized by a number of organizations, including the National Electronic Commerce Coordinating Council (NEC3), which declared:

Regardless of structure, the most critical factor for success [in implementing electronic government] is a clear direction communicated with both authority and responsibility. Responsibility for implementation should rest with an empowered leader, such as the CIO.³

The NEC3 is a coalition among NASIRE, the National Association of Secretaries of State (NASS), the National Association of State Procurement Officials (NASPO), and the National Association of State Auditors, Comptrollers, and Treasurers (NASACT).

Separating technology from government programs is impossible today. State CIOs are responsible for putting their executives’ visions and goals for IT into action. The Harvard Policy Group on Network-Enabled Services and Government, which included CIOs from all levels of government, echoes that sentiment. They define the CIO not solely as a manager of technology, but as a manager of technology “in support of organizational strategy and change management.”⁴ The same sentiment emerges from the private sector as well. Janet Caldw of IBM’s Institute for Electronic Government states:

Our early studies with the Kennedy School of Government revealed that a ‘center of gravity’ for technology policy and strategy is a fundamental critical success factor for governments to move forward aggressively. That can come in the form of a Chief Information Officer (CIO) or a Technology and Policy Advisor to the Chief Executive.⁵

As the “center of gravity” for IT policy, the CIO needs to inspire leaders, including elected and appointed officials as well as front-line managers and staff, to dedicate political capital and other resources to the IT agenda. One powerful dynamic of IT is that it can enable and integrate all government services and initiatives—education, criminal justice, economic development, etc.

² Joshua Dean, “President announces creation of new federal Web portal” *GovExec.com*, 24 June 2000, <<http://www.govexec.com/dailyfed/0600/062600j2.htm>> (31 August 2000).

³ National Electronic Commerce Coordinating Council (NEC3), “Electronic Government: A Blueprint for States,” December 1999, <<http://ec3.org/Blueprintv3.pdf>> (11 April 2000), 11.

⁴ The Harvard Policy Group on Network-Enabled Services and Government, “Eight Imperatives for Leaders in a Networked World,” March 2000, <<http://www.ksg.harvard.edu/stratcom/hpg/>> (31 August 2000), 12.

⁵ Janet Caldw, “The Quest for Electronic Government: A Defining Vision,” July 1999, <<http://www.ieg.ibm.com/leadership/leadershipdefault.html#quest>> (31 August 2000), p. 3.

A CIO is necessary to convene key information stakeholders, develop adaptive architectures that are conducive to sharing, and assess the incumbent risks of exposing information on-line. Then the CIO is needed to moderate the changing interests of diverse stakeholders, enforce standards for sharing, and implement the critical security technologies and processes that can ensure privacy. Only then will government enjoy the full benefits of integration. The IBM Institute predicts, "...governments are saving up to 70% by moving services online compared to the cost of providing the same services over the counter."⁶ But eliminating overhead is only a part of a long-term goal, which is to add value to the business of government by delivering superior information and processes for effective, customer-centric programs and services.

Streamlining business processes with technology allowed the Commonwealth of Kentucky's first CIO, Aldona Valicenti, to leverage \$173 million from the state's budget surpluses for the EMPOWER Kentucky program. That initial investment is expected to return a cumulative benefit of \$550 million in savings to the state's general fund by 2004.⁷ That's money for education, public safety, tax reduction, etc. At the local level, former mayor Stephen Goldsmith established an award-winning digital government for the City of Indianapolis, allowing him save money and provide a wide range of online service to citizens.⁸ The mayor's office of that city includes an office of the CIO. A more recent re-organization in the City of Virginia Beach, Virginia also includes an office of the CIO dedicated to "Organization wide vision setting and business alignment...".⁹

Globally, a number of other nations are taking aggressive approaches to digital government, including the Special Administrative Region of Hong Kong,¹⁰ Singapore,¹¹ Australia,¹² Canada,¹³ the United Kingdom,¹⁴ and the European Union.¹⁵ Australia Online represents a major effort to have all of that nation's services web-enabled by 2001.¹⁶ Australia, Hong Kong, and Singapore have also signed memoranda of understanding to facilitate cross-national e-commerce, underscoring the important role a national digital government can play in facilitating economic growth.¹⁷

In conclusion, let me say that my goals for today have been to reinforce my testimony before this committee from last March. Support for the role of the CIO comes from many quarters.

⁶ Ibid., 6.

⁷ EMPOWER Kentucky, "A Progress Report," January 2000, <<http://empower.state.ky.us/>> (31 August 2000), 2.

⁸ Please see <<http://www.indygov.org/winner.htm>> and Mr. Goldsmith's address in "Creating a Government for the 21st Century," 30 March 2000, <<http://207.120.254.85/lectures.asp>> (31 August 2000).

⁹ Gwen Cowart and David Sullivan, "City of Virginia Beach, VA: Communications and I.T. Re-org White Paper," 01 July 99, <http://www.lgov.org/document/docdetail.asp?doc_id=16> (31 August 2000).

¹⁰ Please see <<http://www.info.gov.hk/eindex.htm>> (31 August 2000).

¹¹ Please see <<http://www.gov.sg/>> (31 August 2000).

¹² Please see <<http://www.fed.gov.au/>> (31 August 2000).

¹³ Please see <http://www.gc.ca/main_e.html> (8 September 2000).

¹⁴ Reuters, "Britain to Deliver All Services Online by 2005" *The Standard*, 30 March 2000, <<http://www.thestandard.com/article/display/0,1151,12564,00.html>> (3 April 2000).

¹⁵ Ibid.

¹⁶ Office of Government Online (OGO), "Strategic Priorities," n.d., <<http://www.govonline.gov.au/projects/strategy/StrategicPriorities.htm>> (31 August 2000).

¹⁷ OGO, "Memoranda of Understanding," n.d., <<http://www.govonline.gov.au/projects/international/mou.htm>> (31 August 2000).

Furthermore, empowered CIOs, such as those in Kentucky and Indianapolis, can achieve much. NASIRE encourages the Federal government to establish an executive office of the CIO. However, we caution that the role of the CIO cannot be defined with one act. The work of the CIO will not end after one project. In our estimation, the future success of any government in the New Economy depends on not only establishing an office of the CIO, but also in constantly evolving the role of the CIO as technologies change and new opportunities emerge. Only then will the full fruition of digital government be within our reach.

NASIRE

Representing Chief Information Officers of the States
2000 Mid-Year Conference
CIO Round Table

Those in attendance:

Aldona Valicenti (KY), Moderator
Mike Benzen (MO)
George Boersma (MI)
Elias Cortez (CA)
Otto Doll (SD)
Charles Gerhards (PA)
Mike Hale (GA)
Don Hutchinson (LA)
Steve Kolodney (WA)
Laura Larimer (IN)
Dave Litchliter (MS)
Marlene Lockard (NV)
Marcia Martinez (NM)
Alisoun Moore (MD)
Wendy Rayner (NJ)
Al Sherwood (for Dave Moon, UT)
Randy von Liski (for Mary Barber Reynolds, IL)
Rick Webb (NC)

Guests:

Thom Rubel, Director, Center for Best Practices, National Governors' Association (NGA)

THE ROLE OF THE STATE CIO

Valicenti welcomed the CIOs and introduced the first topic for discussion—NGA's survey of gubernatorial priorities. The survey covered a wide range of topics and garnered 34 responses from the 55 eligible state and territorial governors. Concerning IT management, 74% of the respondents declared it a high priority. The survey allowed respondents to pick multiple priorities.

Rubel commented that the intent of the survey was to help NGA determine priority issues for its programs. Webb said that North Carolina has moved IT management into the forefront. The state's Senate Bill 222 dramatically reconfigured state management of IT, including budgeting, planning, and procurement, and established the position of CIO. The goal is to break down silos and make the enterprise the central concern. Larimer added that IT management involves more than establishing a position of CIO. That role must be made central to the IT management process and be reinvented over time.

Rubel asked what the threshold would be for determining "real CIO authority." Rayner answered that an effective CIO will have a clear mandate from the governor and access to the

governor's office. That access should represent a "constant dialogue" between the CIO and the governor on IT issues. For a governor to be truly supportive, the CIO must have open access to the governor's office.

Martinez remarked that New Mexico has recently established a true CIO. The position had previously existed only under executive order. She believes that New Mexico plans to make the position one that enjoys direct contact with the governor. Sherwood commented that the formal title of "CIO" is not as important as "statutory, enterprise-wide authority" invested in a CIO-like position. Kolodney added that the CIO must have tangible "resources to bring to the party," which come from having resources to invest in ideas and a reputation for delivering results. He believes that some CIOs have enjoyed intangible benefits that CIOs cannot necessarily control, such as coming from technology-rich regions.

Webb stated that CIOs must have the ability to balance operation and innovation. Change management and the authority to reorient the business culture are integral to the job. Doll commented that CIO should be a peer to the other agency chiefs, including control of IT operating funds, which can relieve some of the need to rely on gubernatorial access. Moore said that the CIO should have authority over the process, including policy and standards development. The CIO should be part of the "governor's team" with a formal role of leadership, not just IT management.

Boersma stated that he is invested with executive authority to oversee all IT projects, while he does not formally report to the governor. He said, "A CIO must have vision, then the governor will see you." The CIO must be willing to make tough decisions when enforcing standards and be able to go with a decision once it's made. Gerhards agreed, saying that a CIO must be empowered to "push back and push back hard" when defending decisions. The agencies must know that "the governor wants it done." Hutchinson added that the CIO must have the respect of peer cabinet secretaries and support from the governor. IT affects economic development and education, which are key goods for the citizens.

Cortez remarked that California has 81 functional CIOs, which makes it important for the state CIO to remain engaged in "mission-critical decision making." Von Liski added that Illinois is considering providing its Chief Technology Officer, with the necessary authority to oversee policy and vision development, procurement, as well as centralized operations and budgeting. Litchlitter said that budgeting in Mississippi is a challenge as his office is a fully reimbursable agency that must fund itself, which makes it difficult for him to get the necessary funds "to get out front on innovation."

Valicenti asked for the essential characteristics for a CIO. Rayner said the CIO must sit on the governor's cabinet. Larimer offered that the CIO should have access to the governor's key staff and be a part of the weekly meeting of the governor's advisors. Doll agreed that the CIO should be on a peer level with cabinet officers. Moore commented that many state CIOs will have to live with multiple bosses as they sit under cabinet secretaries. Webb concurred that directly reporting to the governor would be nice, but, being under a cabinet officer, he must manage six to eight bosses at all times, which leads to more time spent "keeping everyone on board."

Moore said that economic development and education are priority concerns for improving the standard of living for citizens. Valicenti said that her job is about aligning government with the business needs of the citizens. The CTO handles the operational and telecommunications concerns. Larimer added that she is involved with high-tech commercial

development, saying, “You can’t attract high-tech businesses without a high-tech state to support them.”

Boersma stated that his roles are to (1) put governance in place to fulfill the executive order for enterprise control, (2) oversee methods and standards through the project management office, (3) oversee strategy through the office of IT solutions, (4) provide centralized computer services for state agencies, and (5) assess agency IT through benchmarking, which will move the infrastructure toward the state’s e-commerce vision.

Kolodney commented that, as a cabinet level department, his office oversees telecommunications (voice and data) and providing discretionary services to other agencies on a competitive basis. His agency receives no appropriation. His Information Services Board is chaired by the governor’s chief of staff. The board includes higher education and the courts among others. He believes that being self-funded keeps the agency disciplined. Webb agreed with Washington’s approach, saying that IT services must have “mass-market appeal.” North Carolina works with a management commission and an association of state IT industries. He finds that metrics keep the pressure on the agency to perform.

Valicenti asked which one change would the CIOs most like to make to their jobs. Gerhards answered that he would eliminate the agency concept—declare one, unified state government that works for the citizens. It would be functional and responsive. He said that this arrangement is the only choice or more problems for government will lie ahead. Sherwood said he would have the federal government interact with the states on a functional basis, much like the block grant arrangements. Webb said he would institute incentives for performance. Government presently offers high risk with low rewards. He would reward employees for decision making and pay for performance.

Boersma asserted that removing cultural barriers would be his choice. Moore agreed with Webb’s desire to revise personnel compensation to make it more competitive. Von Liski would implement faster procurement processes to align with the technology cycle and allow decisions to be based on state-vendor relationships. Litchliter said he would establish a technology innovation fund to provide incentives to agencies.

Valicenti added that the Gartner Group found e-commerce to be the number one issue in the states followed by personnel recruitment and retention. She mentioned that states and vendors have been accused of “hyping” IT in relation to digital government. She asked if e-government was going to fall by the wayside as artificial intelligence and code generation have. Boersma answered that digital government will happen “because the taxpayers demand it.” Doll agreed that it will happen in some form, but he is unsure whether digital government can achieve the expectation of eliminating paper-based procedures. He does not want to see digital government compared to education where money is poured in without conclusive evidence of success—for example, higher SAT scores—and most success stories are anecdotal.

Webb concurred with Boersma that the movement is “from the outside in.” He advised states to “be bold and go all the way.” States will have to reallocate staff, partner with the private sector, and pursue “hard-line changes, not instant gratification.” States will need to revise their financial infrastructure. The heat will be increasing. “Those who are out ahead right now,” he said, “will soon be reactive, if they don’t continue to innovate.” Kolodney commented that these are the best of times. “All doors are open for change. The future of digital government is ours to win or lose,” he added. Moore commented that states will need to manage public expectations and define success before they reach for it.

Valicenti asked how states will re-engineer. Rubel responded that the American system of government was designed to be slow and asked if the governor's recognize this when it comes to implementation of digital government. Boersma said his governor wants to re-engineer for e-government and that it won't be easy. "We'll face more internal than external obstacles," said Boersma. Moore said it comes down to leadership. Maryland implemented on-line licensing renewal and staff were reallocated as the workload decreased.

The CIOs were asked how they would deal with citizens resistant to on-line transaction. Moore answered that services will continue to be delivered in a variety of modes with some of those modes shrinking away. Larimer said that the political reality will redirect some concerns. Some private sector firms are mandating direct payroll deposits with e-mail confirmations. State government might do the same with its employees, and eventually move to electronic transactions with other recipients of state funds, but not soon. Kolodney asserted that these are the best of times for CIOs. "All the doors are open. We have a profound opportunity to fundamentally change government. It's ours to win or lose."

The CIOs were asked what the role of vendors should be with state legislators. Larimer answered that vendors should not "surprise me" with their lobbying activities. Doll said he encourages vendors to help in educate legislators on how to explain the benefits of technology to their constituents.

Rubel asked Kolodney to explain Washington's recent order on privacy. Kolodney answered that the order was in response to the easy availability of electronic information. The governor issued an executive order in lieu of legislative action. A notice will be posted on all sites where agencies collect information. The state forbids multiple reuse of information by vendors downstream. Privacy is the priority issue for the attorney's general. Sherwood added that the National Electronic Commerce Coordinating Council (NEC3) has done a good job addressing the issue. He said the states must address the issue with a policy that allows personalization of privacy levels. Hutchinson asked how many CIOs have input on state privacy policies. Several responded that they do. Sherwood commented that privacy laws have been so broad that they were defeated in many states. Moore said that privacy must be part of an overall IT package that includes the CIO as a caretaker of information. The agencies must be held responsible for where information goes and citizens need on/off control of access to their records. Kolodney added that Washington does not sell data.

IN HOUSE

1998 REGULAR SESSION

HOUSE BILL NO. 789

MONDAY, MARCH 2, 1998

Representative Marshall Long introduced the following bill which was ordered to be printed.

AN ACT relating to the establishment of the chief information officer for the executive branch of the Commonwealth.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

SECTION 1. A NEW SECTION OF KRS CHAPTER 61 IS CREATED TO READ AS FOLLOWS:

The General Assembly finds and declares that:

(1) The establishment of the Office of the Chief Information Officer as the Commonwealth's single point of contact and spokesperson for all matters related to information technology and resources, including policies, standard setting, deployment, strategic and tactical planning, acquisition, management, and operations is necessary and in keeping with the industry trends of the private and public sectors;

(2) The appropriate use of information technology by the Commonwealth can improve operational productivity, reduce the cost of government, enhance service to customers, and make government more accessible to the public;

(3) Government-wide planning, investment, protection, and direction for information resources must be enacted to:

(a) Ensure the effective application of information technology on state business operations;

(b) Ensure the quality, security, and integrity of state business operations; and

(c) Provide privacy to the citizens of the Commonwealth;

(4) The Commonwealth must provide information technology infrastructure, technical directions, and a proficient organizational management structure to facilitate the productive application of information technology and resources to accomplish programmatic missions and business goals;

(5) Oversight of large scale and government statewide systems or projects is necessary to protect the Commonwealth's investment and to ensure appropriate

- 1 integration with existing or planned systems;
- 2 (6) A career development plan and professional development program for
 3 information technology staff of the executive branch is needed to provide key
 4 competencies and adequate on-going support for the information resources of the
 5 Commonwealth and to ensure that the information technology staff will be
 6 managed as a Commonwealth resource;
- 7 (7) The Commonwealth is in need of information technology advisory capacities to
 8 the Governor and the agencies of the executive cabinet;
- 9 (8) Appropriate public-private partnerships to supplement existing resources must be
 10 developed as a strategy for the Commonwealth to comprehensively meet its
 11 spectrum of information technology and resource needs; and
- 12 (9) The exercise by the chief information officer of powers and authority conferred
 13 by Sections 1 to 4 of this Act shall be deemed and held to be the performance of
 14 essential governmental functions.

15 SECTION 2. A NEW SECTION OF KRS CHAPTER 61 IS CREATED TO
 16 READ AS FOLLOWS:

17 There is hereby established a position of chief information officer for the
 18 Commonwealth. This position shall be exempt from the classified service under KRS
 19 18A.115 and from the salary limitations of KRS 64.640, and shall be bonded
 20 commensurate with cabinet secretaries under KRS 62.160. The chief information
 21 officer shall be appointed by the Governor and serve in the Governor's Executive
 22 Cabinet. The chief information officer shall report to the secretary of the Governor's
 23 cabinet concerning his or her responsibilities to provide direction, stewardship,
 24 leadership, and general oversight of information technology and information
 25 resources. For purposes of this section, unless the context requires otherwise,
 26 "information technology" and "information resources" shall have the same meaning
 27 as in KRS 61.942.

- 1 (1) The chief information officer shall be the principal adviser to the Governor and
2 the executive cabinet on information technology policy, including policy on the
3 acquisition and management of information technology and resources.
- 4 (2) The chief information officer shall carry out functions necessary for the
5 efficient, effective, and economical administration of information technology and
6 resources within the executive branch. Roles and duties of the chief information
7 officer shall include but not be limited to:
- 8 (a) Developing strategies and policies to support and promote the effective
9 applications of information technology within state government as a means
10 of saving money, increasing employee productivity, and improving state
11 services to the public, including electronic public access to information of
12 the Commonwealth;
- 13 (b) Assessing, recommending, and implementing information technology
14 governance and organization design to include effective information
15 technology personnel management practices;
- 16 (c) Promoting effective and efficient design and operation of all major
17 information resources management processes for executive branch
18 agencies, including improvements to work processes;
- 19 (d) Overseeing and managing strategic information technology directions,
20 standards, and architecture;
- 21 (e) Integrating information technology and resources plans with agency
22 business plans;
- 23 (f) Developing, implementing, and maintaining the technology infrastructure
24 of the Commonwealth;
- 25 (g) Overseeing shared Commonwealth information technology resources and
26 services;
- 27 (h) Performing as the focal point and representative for the Commonwealth in

information technology and related areas with both the public and private sector;

(i) Facilitating and fostering applied research in emerging technologies that offer the Commonwealth innovative business solutions;

(j) Establishing appropriate partnerships and alliances to support the effective implementation of information technology projects in the Commonwealth;

(k) Identifying information technology applications that should be statewide in scope, and ensuring that these applications are not developed independently or duplicated by individual state agencies of the executive branch;

(l) Establishing performance measurement and benchmarking policies and procedures;

(m) Reviewing and overseeing large or complex information technology projects and systems for compliance with statewide strategies, policies, and standards, including alignment with Commonwealth business goals, investment, and other risk management policies. The chief information officer is authorized to grant or withhold approval to initiate these projects;

(n) Preparing annual reports and plans concerning the status and result of the state's specific information technology plans and submitting these annual reports and plans to the governor and the General Assembly;

(o) Integrating information technology resources to provide effective and supportable information technology applications in the Commonwealth;
and

(p) Managing the Office of the Chief Information Officer and its budget.

SECTION 3. A NEW SECTION OF KRS CHAPTER 61 IS CREATED TO
READ AS FOLLOWS:

The chief information officer shall have the power to make and enter into memoranda of agreement and contracts necessary or incidental to the performance of duties and

1 execution of powers, including, but not limited to, agreements or contracts with the
 2 United States, other state agencies, and any governmental subdivision of the
 3 Commonwealth.

4 SECTION 4. A NEW SECTION OF KRS CHAPTER 61 IS CREATED TO
 5 READ AS FOLLOWS:

6 (1) To assist the chief information officer and to provide necessary support as
 7 required to carry out the powers and duties of the chief information officer, the
 8 Office of the Chief Information Officer is hereby established and attached for
 9 administrative purposes to the Office of the Governor.

10 (2) The Office of the Chief Information Officer shall have the authority to solicit,
 11 receive, and consider proposals from any state agency, federal agency, local
 12 government, university, nonprofit organization, private person, or corporation.

13 (3) The Office of the Chief Information Officer may solicit and accept money by
 14 grant, gift, donation, bequest, legislative appropriation, or other conveyance to be
 15 held, used, and applied in accordance with Sections 1 to 4 of this Act.

16 (4) The Office of the Chief Information Officer is hereby designated a state agency
 17 for the receipt of federal funds related to information technology.

18 (5) The Office of the Chief Information Officer may promulgate necessary
 19 administrative regulations in accordance with KRS 13A and suggest necessary
 20 legislative actions for the furtherance of duties of the office.

21 Section 5. KRS 12.020 is amended to read as follows:

22 Departments, program cabinets and their departments, and the respective major
 23 administrative bodies that they include are enumerated in this section. It is not intended
 24 that this enumeration of administrative bodies be all-inclusive. Every authority, board,
 25 bureau, interstate compact, commission, committee, conference, council, office, or any
 26 other form of organization shall be included in or attached to the department or program
 27 cabinet in which they are included or to which they are attached by statute or statutorily-

1 authorized executive order; except in the case of the Personnel Board and where the
2 attached department or administrative body is headed by a constitutionally elected officer,
3 the attachment shall be solely for the purpose of dissemination of information and
4 coordination of activities and shall not include any authority over the functions, personnel,
5 funds, equipment, facilities, or records of the department or administrative body.

6 I. Cabinet for General Government - Departments headed by elected officers:

- 7 1. The Governor.
- 8 2. Lieutenant Governor.
- 9 3. Department of State.
 - 10 (a) Secretary of State.
 - 11 (b) Board of Elections.
 - 12 (c) Registry of Election Finance.
- 13 4. Department of Law.
 - 14 (a) Attorney General.
- 15 5. Department of the Treasury.
 - 16 (a) Treasurer.
- 17 6. Department of Agriculture.
 - 18 (a) Commissioner of Agriculture.
 - 19 (b) Kentucky Council on Agriculture.
- 20 7. Superintendent of Public Instruction.
- 21 8. Auditor of Public Accounts.
- 22 9. Railroad Commission.

23 II. Program cabinets headed by appointed officers:

- 24 1. Justice Cabinet:
 - 25 (a) Department of State Police.
 - 26 (b) Department of Criminal Justice Training.
 - 27 (c) Department of Corrections.

- 1 (d) Department of Juvenile Justice.
- 2 (e) Office of the Secretary.
- 3 (f) Offices of the Deputy Secretaries.
- 4 (g) Office of General Counsel.
- 5 (h) Medical Examiner Program.
- 6 (i) Parole Board.
- 7 (j) Kentucky State Corrections Commission.
- 8 (k) Commission on Correction and Community Service.
- 9 2. Education, Arts, and Humanities Cabinet:
- 10 (a) Department of Education.
- 11 (1) Kentucky Board of Education.
- 12 (2) Education Professional Standards Board.
- 13 (b) Department for Libraries and Archives.
- 14 (c) Kentucky Arts Council.
- 15 (d) Kentucky Educational Television.
- 16 (e) Kentucky Historical Society.
- 17 (f) Kentucky Teachers' Retirement System Board of Trustees.
- 18 (g) Kentucky Center for the Arts.
- 19 (h) Kentucky Craft Marketing Program.
- 20 (i) Kentucky Commission on the Deaf and Hard of Hearing.
- 21 (j) Governor's Scholars Program.
- 22 (k) Governor's School for the Arts.
- 23 (l) Office of Development.
- 24 (m) Kentucky Heritage Council.
- 25 (n) Kentucky African-American Heritage Commission.
- 26 3. Natural Resources and Environmental Protection Cabinet:
- 27 (a) Environmental Quality Commission.

- 1 (b) Kentucky Nature Preserves Commission.
- 2 (c) Department for Environmental Protection.
- 3 (d) Department for Natural Resources.
- 4 (e) Department for Surface Mining Reclamation and Enforcement.
- 5 (f) Office of Legal Services.
- 6 (g) Office of Communications and Community Affairs.
- 7 4. Transportation Cabinet:
- 8 (a) Department of Highways.
- 9 (b) Department of Vehicle Regulation.
- 10 (c) Department of Administrative Services.
- 11 (d) Department of Fiscal Management.
- 12 (e) Department of Rural and Municipal Aid.
- 13 (f) Office of Aeronautics.
- 14 (g) Office of General Counsel.
- 15 (h) Office of Public Relations.
- 16 (i) Office of Personnel Management.
- 17 (j) Office of Minority Affairs.
- 18 (k) Office of Environmental Affairs.
- 19 5. Cabinet for Economic Development:
- 20 (a) Department of Administration and Support.
- 21 (b) Department of Job Development.
- 22 (c) Department of Financial Incentives.
- 23 (d) Department of Community Development.
- 24 (e) Tobacco Research Board.
- 25 (f) Kentucky Economic Development Finance Authority.
- 26 6. Public Protection and Regulation Cabinet:
- 27 (a) Public Service Commission.

- 1 (b) Department of Insurance.
- 2 (c) Department of Housing, Buildings and Construction.
- 3 (d) Department of Financial Institutions.
- 4 (e) Department of Mines and Minerals.
- 5 (f) Department of Public Advocacy.
- 6 (g) Department of Alcoholic Beverage Control.
- 7 (h) Kentucky Racing Commission.
- 8 (i) Board of Claims.
- 9 (j) Crime Victims Compensation Board.
- 10 (k) Kentucky Board of Tax Appeals.
- 11 (l) Backside Improvement Commission.
- 12 7. Cabinet for Human Resources:
- 13 (a) Department for Health Services.
- 14 (b) Department for Social Insurance.
- 15 (c) Department for Social Services.
- 16 (d) Department for Medicaid Services.
- 17 (e) Department for Mental Health and Mental Retardation Services.
- 18 (f) Commission for Children with Special Health Care Needs.
- 19 (g) Public Assistance Appeals Board.
- 20 (h) Office of Administrative Services.
- 21 (i) Office of Communications.
- 22 (j) Office of General Counsel.
- 23 (k) Office of Inspector General.
- 24 (l) Office of Policy and Budget.
- 25 (m) Office of the Ombudsman.
- 26 8. Finance and Administration Cabinet:
- 27 (a) Office of Legal and Legislative Services.

- 1 (b) Office of Management and Budget.
- 2 (c) Office of Financial Management and Economic Analysis.
- 3 (d) Office of the Controller.
- 4 (e) Department for Administration.
- 5 (f) Department of Facilities Management.
- 6 (g) Department of Information Systems.
- 7 (h) State Property and Buildings Commission.
- 8 (i) Kentucky Pollution Abatement Authority.
- 9 (j) Kentucky Savings Bond Authority.
- 10 (k) Deferred Compensation Systems.
- 11 (l) Office of Equal Employment Opportunity Contract Compliance.
- 12 (m) Capital Plaza Authority.
- 13 (n) County Officials Compensation Board.
- 14 (o) Kentucky Employees Retirement Systems.
- 15 (p) Commonwealth Credit Union.
- 16 (q) State Investment Commission.
- 17 (r) Kentucky Housing Corporation.
- 18 (s) Governmental Services Center.
- 19 (t) Kentucky Local Correctional Facilities Construction Authority.
- 20 (u) Kentucky Turnpike Authority.
- 21 (v) Historic Properties Advisory Commission.
- 22 9. Labor Cabinet:
- 23 (a) Department of Workplace Standards.
- 24 (b) Department of Workers' Claims.
- 25 (c) Kentucky Labor-Management Advisory Council.
- 26 (d) Occupational Safety and Health Standards Board.
- 27 (e) Prevailing Wage Review Board.

- 1 (f) Workers' Compensation Board.
- 2 (g) Kentucky Employees Insurance Association.
- 3 (h) Apprenticeship and Training Council.
- 4 (i) State Labor Relations Board.
- 5 (j) Kentucky Occupational Safety and Health Review Commission.
- 6 (k) Office of Administrative Services.
- 7 (l) Office of Labor Management Relations.
- 8 (m) Office of General Counsel.
- 9 (n) Workers' Compensation Funding Commission.
- 10 (o) Employers Mutual Insurance Authority.
- 11 10. Revenue Cabinet:
- 12 (a) Department of Property Taxation.
- 13 (b) Department of Compliance and Taxpayer Assistance.
- 14 (c) Department of Administrative Services.
- 15 (d) Office of General Counsel.
- 16 11. Tourism Cabinet:
- 17 (a) Department of Travel Development.
- 18 (b) Department of Parks.
- 19 (c) Department of Fish and Wildlife Resources.
- 20 (d) Kentucky Horse Park Commission.
- 21 (e) State Fair Board.
- 22 (f) Office of Administrative Services.
- 23 (g) Office of Film Promotion.
- 24 (h) Office of General Counsel.
- 25 12. Cabinet for Workforce Development:
- 26 (a) Department for Adult Education and Literacy.
- 27 (b) Department for Technical Education.

- 1 (c) Department of Vocational Rehabilitation.
- 2 (d) Department for the Blind.
- 3 (e) Department for Employment Services.
- 4 (f) State Board for Adult and Technical Education.
- 5 (g) Governor's Council on Vocational Education.
- 6 (h) The State Board for Proprietary Education.
- 7 (i) The Foundation for Adult Education.
- 8 (j) The Kentucky Job Training Coordinating Council.
- 9 (k) Office of General Counsel.
- 10 (l) Office of Communication Services.
- 11 (m) Office of Development and Industry Relations.
- 12 (n) Office of Workforce Analysis and Research.
- 13 (o) Office for Administrative Services.
- 14 (p) Office for Policy, Budget, and Personnel.
- 15 (q) Unemployment Insurance Commission.
- 16 III. Other departments headed by appointed officers:
- 17 1. Department of Military Affairs.
- 18 2. Department of Personnel.
- 19 3. Council on Postsecondary Education.
- 20 (a) Kentucky Community Service Commission.
- 21 4. Department of Local Government.
- 22 5. Kentucky Commission on Human Rights.
- 23 6. Kentucky Commission on Women.
- 24 7. Department of Veterans' Affairs.
- 25 8. Kentucky Commission on Military Affairs.
- 26 9. Office of the Chief Information Officer.
- 27 Section 6. KRS 12.023 is amended to read as follows:

1 The following organizational units and administrative bodies shall be attached to the Office
2 of the Governor:

- 3 (1) Council on Postsecondary Education;
- 4 (2) Department of Military Affairs;
- 5 (3) Department of Local Government;
- 6 (4) Kentucky Commission on Human Rights;
- 7 (5) Kentucky Commission on Women;
- 8 (6) Kentucky Commission on Military Affairs; ~~and~~
- 9 (7) Coal Marketing and Export Council; and
- 10 (8) Office of the Chief Information Officer.

11 Section 7. KRS 18A.115 is amended to read as follows:

- 12 (1) The classified service to which KRS 18A.005 to 18A.200 shall apply shall comprise
13 all positions in the state service now existing or hereafter established, except the
14 following:
 - 15 (a) The General Assembly and employees of the General Assembly, including the
16 employees of the Legislative Research Commission;
 - 17 (b) Officers elected by popular vote and persons appointed to fill vacancies in
18 elective offices;
 - 19 (c) Members of boards and commissions;
 - 20 (d) Officers and employees on the staff of the Governor, the Lieutenant Governor,
21 the Office of the secretary of the Governor's Cabinet, and the Office of
22 Program Administration;
 - 23 (e) Cabinet secretaries, commissioners, office heads, and the administrative heads
24 of all boards and commissions, including the executive director of Kentucky
25 Educational Television;
 - 26 (f) Employees of Kentucky Educational Television who have been determined to
27 be exempt from classified service by the Kentucky Authority for Educational

- 1 Television, which shall have sole authority over such exempt employees for
2 employment, dismissal, and setting of compensation, up to the maximum
3 established for the executive director and his principal assistants;
- 4 (g) One (1) principal assistant or deputy for each person exempted under
5 subsection (1)(e) of this section;
- 6 (h) One (1) additional principal assistant or deputy as may be necessary for making
7 and carrying out policy for each person exempted under subsection (1)(e) of
8 this section in those instances in which the nature of the functions, size, or
9 complexity of the unit involved are such that the commissioner approves such
10 an addition on petition of the relevant cabinet secretary or department head
11 and such other principal assistants, deputies, or other major assistants as may
12 be necessary for making and carrying out policy for each person exempted
13 under subsection (1)(e) of this section in those instances in which the nature of
14 the functions, size, or complexity of the unit involved are such that the board
15 may approve such an addition or additions on petition of the department head
16 approved by the commissioner;
- 17 (i) Division directors subject to the provisions of KRS 18A.170. Division
18 directors in the classified service as of January 1, 1980, shall remain in the
19 classified service;
- 20 (j) Physicians employed as such;
- 21 (k) One (1) private secretary for each person exempted under subsection (1)(e),
22 (g), and (h) of this section;
- 23 (l) The judicial department, referees, receivers, jurors, and notaries public;
- 24 (m) Officers and members of the staffs of state universities and colleges and
25 student employees of such institutions; officers and employees of the Teachers'
26 Retirement System; and officers, teachers, and employees of local boards of
27 education;

- 1 (n) Patients or inmates employed in state institutions;
- 2 (o) Persons employed in a professional or scientific capacity to make or conduct a
- 3 temporary or special inquiry, investigation, or examination on behalf of the
- 4 General Assembly, or a committee thereof, or by authority of the Governor,
- 5 and persons employed by state agencies for a specified, limited period to
- 6 provide professional, technical, scientific, or artistic services under the
- 7 provisions of KRS 45A.690 to 45A.725;
- 8 (p) Seasonal, temporary, and emergency employees;
- 9 (q) Federally funded time-limited employees;
- 10 (r) Officers and members of the state militia;
- 11 (s) State Police troopers and sworn officers in the Department of State Police,
- 12 Justice Cabinet;
- 13 (t) University or college engineering students or other students employed part-
- 14 time or part-year by the state through special personnel recruitment programs;
- 15 provided that while so employed such aides shall be under contract to work
- 16 full-time for the state after graduation for a period of time approved by the
- 17 commissioner or shall be participants in a cooperative education program
- 18 approved by the commissioner;
- 19 (u) Superintendents of state mental institutions, including heads of mental
- 20 retardation centers, and penal and correctional institutions as referred to in
- 21 KRS 196.180(2);
- 22 (v) Staff members of the Kentucky Historical Society, if they are hired in
- 23 accordance with KRS 171.311;
- 24 (w) County and Commonwealth's attorneys and their respective appointees;
- 25 (x) Chief district engineers and the state highway engineer;
- 26 (y) Veterinarians employed as such by the Kentucky State Racing Commission or
- 27 the Kentucky Harness Racing Commission;

- 1 (z) Employees of the Kentucky Peace Corps; ~~and~~
- 2 (aa) Employees of the Council on Postsecondary Education; and
- 3 (bb) Chief Information Officer of the Commonwealth.
- 4 (2) Nothing in KRS 18A.005 to 18A.200 is intended, or shall be construed, to alter or
- 5 amend the provisions of KRS 150.022 and 150.061.
- 6 (3) Nothing in KRS 18A.005 to 18A.200 is intended or shall be construed to affect any
- 7 nonmanagement, nonpolicy-making position which must be included in the classified
- 8 service as a prerequisite to the grant of federal funds to a state agency.
- 9 (4) Career employees within the classified service promoted to positions exempted from
- 10 classified service shall, upon termination of their employment in the exempted
- 11 service, revert to a position in that class in the agency from which they were
- 12 terminated if a vacancy in that class exists. If no such vacancy exists, they shall be
- 13 considered for employment in any vacant position for which they were qualified
- 14 pursuant to KRS 18A.130 and 18A.135.
- 15 (5) Nothing in KRS 18A.005 to 18A.200 shall be construed as precluding appointing
- 16 officers from filling unclassified positions in the manner in which positions in the
- 17 classified service are filled except as otherwise provided in KRS 18A.005 to
- 18 18A.200.
- 19 (6) The positions of employees who are transferred, effective July 1, 1998, from the
- 20 Cabinet for Workforce Development to the Kentucky Community and Technical
- 21 College System shall be abolished and the employees' names removed from the
- 22 roster of state employees. Employees that are transferred, effective July 1, 1998, to
- 23 the Kentucky Community and Technical College System under KRS Chapter 164
- 24 shall have the same benefits and rights as they had under KRS Chapter 18A and have
- 25 under KRS 164.5805; however, they shall have no guaranteed reemployment rights
- 26 in the KRS Chapter 151B or KRS Chapter 18A personnel systems. An employee
- 27 who seeks reemployment in a state position under KRS Chapter 151B or KRS

1 Chapter 18A shall have years of service in the Kentucky Community and Technical
2 College System counted towards years of experience for calculating benefits and
3 compensation.

4 Section 8. KRS 42.029 is amended to read as follows:

- 5 (1) There is established a department of state government to be known as the
6 Department of Information Systems. The department shall be a part of the Finance
7 and Administration Cabinet. The Department of Information Systems shall be
8 headed by a commissioner, appointed by the secretary of the Finance and
9 Administration Cabinet, with the approval of the Governor. The commissioner shall
10 be responsible to the secretary.
- 11 (2) The secretary of the Finance and Administration Cabinet shall appoint, with the
12 approval of the Governor, a deputy commissioner of the Department of Information
13 Systems, pursuant to KRS 12.050. The commissioner of information systems, with
14 the approval of the secretary of the Finance and Administration Cabinet, may
15 appoint such principal assistants, pursuant to KRS 12.050, as may be necessary for
16 the development and implementation of policy. The commissioner may employ,
17 pursuant to the provisions of KRS Chapter 18A, such personnel as may be necessary
18 to execute the functions and duties of the department.
- 19 (3) The Department of Information Systems shall provide ~~leadership, policy direction,~~
20 ~~and~~ technical support and services to all executive agencies of state government in
21 the application of information technology. The department shall:
- 22 (a) Assure compatibility ~~[portability]~~ and connectivity of Kentucky's information
23 systems; and
- 24 (b) Implement necessary management processes to assure full compliance with the
25 Kentucky information resources architecture as adopted by the Kentucky
26 Information Resources Management Commission.
- 27 (4) The Department of Information Systems shall include the following divisions, each

1 of which shall be headed by a director appointed by the secretary with the approval
2 of the Governor, pursuant to KRS 12.050:

- 3 (a) The Division of Network Services, which shall be responsible for network
4 planning, network design, network management, systems administration,
5 research and evaluation of desktop and departmental computer technologies,
6 support for end user computing, and information dissemination;
- 7 (b) The Division of Computer Services, which shall be responsible for all
8 computer operations, systems programming, technical support services, data
9 storage, and database management services;
- 10 (c) The Division of Systems Development, which shall be responsible for
11 providing comprehensive systems analysis, design, and development services,
12 and applications consulting services to designated state agencies with primary
13 responsibility for supporting economic development, education, human
14 services, and public protection systems;
- 15 (d) The Division of Systems Engineering, which shall be responsible for providing
16 comprehensive systems analysis, design, and development services and
17 applications consulting services to designated state agencies with primary
18 responsibility for supporting environmental, financial, labor, personnel,
19 revenue, safety, justice, tourism, and transportation systems; and
- 20 (e) The Division of Support Services, which shall be responsible for planning and
21 procurement assistance, fiscal administration, service coordination, application
22 development standards, data security, disaster recovery planning, technical
23 training, technical publications, and facilities support.
- 24 (f) The secretary of the Finance and Administration Cabinet, in consultation with
25 the commissioner of the Department of Information Systems, shall designate
26 the state agencies to be provided services by the Division of Systems
27 Development and the Division of Systems Engineering based on the

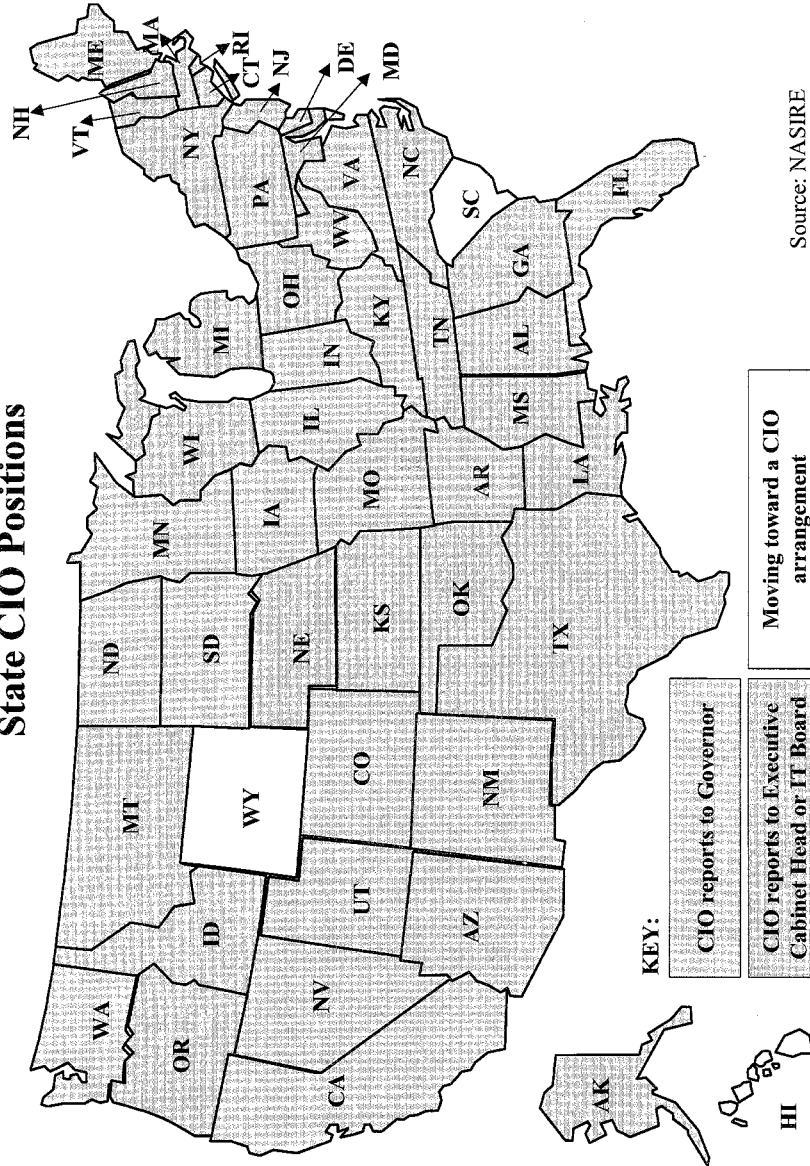
- 1 complexity of the services to be provided and each division's work load.
- 2 (5) The Department of Information Systems may delegate authority to individual state
3 agencies for the performance of departmental and desktop level functions if the
4 commissioner finds the delegation to be in the best interest of the Commonwealth.
5 All delegations of authority shall:
- 6 (a) Be in written form;
- 7 (b) Specify the level and scope of functions to be performed; and
- 8 (c) Provide notice to the agency receiving delegation of authority, that the
9 delegated authority will be revoked if the commissioner finds that the functions
10 being performed fail to adhere to prescribed criteria or if the commissioner
11 finds that it is no longer in the best interest of the Commonwealth to continue
12 the agency's delegation of authority. Nothing in this subsection shall apply to
13 the data processing operations or personnel of the Kentucky Retirement
14 Systems or the Kentucky Teachers' Retirement System.
- 15 (6) The Department of Information Systems may provide general consulting services,
16 technical training, and support for generic software applications, upon request from
17 a local government, if the commissioner finds that the requested services can be
18 rendered within the established terms of the federally approved cost allocation plan.
- 19 (7) Nothing in this section shall be construed to alter or diminish the provisions of KRS
20 171.410 to 171.740 or the authority conveyed by these statutes to the Archives and
21 Records Commission and the Department for Libraries and Archives.
- 22 (8) The department may promulgate necessary administrative regulations for the
23 furtherance of this section.
- 24 Section 9. KRS 61.945 is amended to read as follows:
- 25 (1) There is hereby created an independent agency of state government to be known as
26 the Kentucky Information Resources Management Commission, hereafter called the
27 "commission." It shall be the responsibility of the commission to coordinate and

- 1 guide the application of information technologies and resources in the executive
2 branch of state government.
- 3 (2) The commission shall consist of:
- 4 (a) Three (3) cabinet secretaries from the executive branch, at least one (1) of
5 whom shall be from either the Transportation or Human Resources Cabinet,
6 appointed by the Governor, or their respective designees;
- 7 (b) The state budget director or his designee;
- 8 (c) The commissioner of the Department of Information Systems;
- 9 (d) The State Librarian or his designee;
- 10 (e) One (1) representative from the public universities to be appointed by the
11 Governor from a list of three (3) persons submitted by the president of the
12 Council on Postsecondary Education;
- 13 (f) Two (2) citizen members from the private sector with information resources
14 management knowledge and experience to be appointed by the Governor;
- 15 (g) One (1) representative of local government appointed by the Governor from a
16 list of six (6) persons, three (3) to be submitted by the president of the
17 Kentucky League of Cities, and three (3) to be submitted by the president of
18 the Kentucky Association of Counties;
- 19 (h) One (1) member of the press to be appointed by the Governor from a list of
20 three (3) persons submitted by the president of the Kentucky Press
21 Association;
- 22 (i) The executive director of the Kentucky Authority for Educational Television;
- 23 (j) The chairman of the Communications Advisory Council as an ex officio;
24 ~~nonvoting~~ member; ~~and~~
- 25 (k) The chairman of the Geographic Information Advisory Council as an ex
26 officio; ~~nonvoting~~ member; and
- 27 (l) The Chief Information Officer of the Commonwealth.

- 1 (3) The commission shall select from its membership a chairperson and any other
2 officers it considers essential. A member of the commission shall not:
- 3 (a) Be an officer, employee, registered legislative agent, Executive Branch
4 lobbyist, or paid consultant of a business entity that has, or of a trade
5 association for business entities that has, a substantial interest in the
6 information resources technology industry;
- 7 (b) Own, control, or have directly or indirectly, more than a ten percent (10%)
8 interest in a business entity that has a substantial interest in the information
9 resources technology industry;
- 10 (c) Be in any manner connected with any contract or bid for furnishing any state
11 governmental body with information resources systems, the computers on
12 which they are automated, or a service related to information resources
13 systems; or
- 14 (d) Receive anything of value from an individual, firm, or corporation to whom a
15 contract may be awarded, directly or indirectly, by rebate, gift, or otherwise.
- 16 (4) (a) It shall be a ground for removal of a member of the commission if the member:
- 17 1. Does not maintain during service on the commission the qualifications or
18 status required for initial appointment to the commission;
- 19 2. Violates a prohibition established by subsection (3) of this section; or
- 20 3. Is absent from three (3) consecutive meetings or more than half of the
21 regularly-scheduled commission meetings that the member is eligible to
22 attend during a state fiscal year unless the absence is excused by majority
23 vote of the commission.
- 24 (b) The validity of an action of the commission shall not be affected by the fact
25 that it was taken when a ground for removal of a member existed. If the
26 chairperson of the commission has knowledge that a potential ground for
27 removal of a commission member exists, the chairperson shall notify the

- 1 Governor of the potential ground for removal.
- 2 (5) (a) The term of office of the members specified in subsection (2)(b), (c), (d), (i),
3 (j), and (k) of this section shall be the same as the term of office by virtue of
4 which they serve upon the commission.
- 5 (b) The terms of the cabinet secretaries appointed pursuant to subsection (2)(a) of
6 this section shall be established in the commission's operating policies or
7 bylaws not to be less than two (2) years.
- 8 (6) Members of the commission appointed pursuant to subsection (2)(e), (f), (g), and (h)
9 of this section shall serve for a term of four (4) years. Vacancies in the membership
10 of the commission shall be filled in the same manner as the original appointments. If
11 a nominating organization changes its name, the subsequent organization having the
12 same responsibilities and purposes shall be the nominating organization.
- 13 (7) Members of the commission shall serve without compensation, but shall be
14 reimbursed for actual expenses incurred in the performance of their duties.
- 15 (8) A majority of the members shall constitute a quorum for the transaction of business.
16 Members' designees shall have voting privileges at commission meetings.

State CIO Positions



Mr. HORN. Thank you very much. We appreciated that testimony Mr. Doll. I'm going to have to do something I don't like doing because I'm going to have to interject for a question period before the representative of the administration has to go, and she said she has to go at 11:15 and I want Mr. Davis, Mr. Turner to question her before now and 11:15. So I first yield for questions 5 minutes for the gentleman from Virginia, Mr. Davis.

Mr. DAVIS. Thank you. Sally, thanks for being here once again and for all the work you're doing. In your written testimony you offer that Clinger-Cohen is correct in placing centralized leadership responsibilities for IT investment management within OMB because OMB has budget and program oversight responsibilities throughout the executive branch and can work to ensure that IT supports agency missions and policies. You go on to say that legislation which mandates a particular approach may lock in oversight structures and constrain our capacity to solve the problems that are unknown to us today.

I wonder if you could take a minute and describe the leadership role that OMB has displayed in the past in defining and managing interagency items, not just speaking to money items but managing IT resources. How does OMB keep track of those initiatives so that responsible decisions can be made when projects are not working and should be halted or a new direction should be taken? Can you give me a feel for how that works?

Ms. KATZEN. Sure. Thank you. In one respect we take our management challenges each year as part of the budget. We prepare those priority management objectives, we call them, the PMOs, that warrant senior management attention, and IT management is always on the list. This year I think we have four that include that. People are assigned within OMB both in the statutory offices and in the RMOs, the Resource Management Offices, which do the budgeting and management hands, often to report on a monthly basis on the progress made. I have prepared this report for the Director, for the President and see how we are proceeding on the most important challenges.

At the other end of the spectrum OMB is actually a fairly lean and mean organization—well, I'm not so sure it's mean but it is lean. We only have about 500 people for all the governmentwide functions. We leverage our power and authority through interagency councils, whether it's the Statistical Policy Council which was created and reports through the Chief Statistician of the United States, who's in the Office of Administration. In the Office of Information, Regulatory Affairs, or the CIO Council, the Deputy Director for Management, me now, sits as chair of the CIO Council, sits as chair of the CFO Council, that's the Chief Financial Officers, sits as chair of the PCIE, which is the President's Committee on Integrity and Efficiency, which are the IGs, the Procurement Executives Council. What I have done—

Mr. HORN. Excuse me. Could you sort of spell it out for the people that are listening?

Ms. KATZEN. CIO Council is the Chief Information Officers Council. CFO Council is the Chief Financial Officers Council. The PEC is the Procurement Executives Council. The PCIE is the President's

Council on Efficiency and Integrity, which is the IGs, which are the Inspector Generals.

Each of these councils have committees. Mr. Flyzik indicated the myriad numbers of committees that they have. Their e-government committee representative meets with me, with the CFO Council e-government representative and the PEC e-government representative, at least once a month, where we sort through priorities, we hear about initiatives. And the CFO Council people will sit there and say, oh, is that what the CIO Council is doing? Isn't that interesting? We're able to exchange best practices. Mr. Flyzik has attended those meetings in the past. That's another way we leverage.

Mr. DAVIS. Where is the decisionmaking authority after you all sit down and you go through all these? Does it come to you then up through the head of OMB in terms of resolving—

Ms. KATZEN. In most instances it's not a decision that has to be made yes or no. It's a sorting through priorities. But if there were, it would be through me and I would consult with Jack Lew, the Director, or the President or Vice President. Mr. Doll was talking about the President's interest in FirstGov. We presented it to him and he loved it, and he therefore announced it. It was something we had developed, and we had developed it with the help of the CIO Council as well as the PEC Council because one piece of this FirstGov is to have a single gateway for procurement for buying and selling to the government, and they're interested in that aspect of it.

So we put all these pieces together. When we presented it to the President he was most enthusiastic about it. So it can go at different levels, in part depending upon how radical it may be or how much funding is necessary.

And there's also, one of the problems that we've had, and I've heard this from a number of the people who are talking about this, is the funding. OMB has included requests for funding for security, for e-government, for digital signatures, for a variety of things and we just were hoping that the Congress will be more receptive to those requests.

Mr. DAVIS. I think my 5 minutes are up. I want to make sure—I might want to give you a couple of written questions, but I think you've given me the outlines.

Ms. KATZEN. Be happy to supply any answers to that. Thank you very much, sir.

Mr. HORN. The gentleman from Texas, Mr. Turner, 5 minutes for questioning the witness.

Mr. TURNER. Thank you, Mr. Chairman. We appreciate all of your input on this issue, and as you know, in our meetings together there are some issues that must be resolved before we can move forward. And obviously we want to be sure we structure this new Chief Information Officer in a way that's consistent with the roles that you are accustomed to having oversight over. I did notice that in a letter that we received just yesterday from Mr. Gilligan, who is the CIO of the Department of Energy, he said that only a small portion of the funding requests we're talking about for information technology funding is intended to provide for coordinating governmentwide security efforts.

We were talking yesterday, as you know, about computer security as well as providing common solutions that will improve efficiency and effectiveness of individual agency security programs. He goes on to say these initiatives are not designed to replace individual agency programs already in place. Rather, they seek to build on their successes and expand existing infrastructure. In an attachment to his letter he says most of the funding that has been provided in the Federal budget has been directed at the individual agencies. He says, and I quote, only a small portion of this funding request is intended to provide for cross government initiatives.

I'd like for you to describe for us some specific cross agency initiatives relating to information technology that OMB has successfully implemented.

Ms. KATZEN. I will start by noting that I don't completely agree with his characterization of the way we do the funding. It is true that there is a relatively small portion that is designed for intra—interagency, among agencies, cross-cutting, governmentwide types of projects. But the security, for example, should be built into the system. It shouldn't be a separate kind of venture. It should be part of the capital planning process, and that's one of the things we're working on.

But having said that, in terms of the types of activities that we have, 2 years ago the Congress and Treasury-Postal gave us a \$7 million fund for us to allocate for governmentwide efforts, and that money was used in part for the CIO Council, and we asked them to come up with their wish list, their priorities, so that we could be responsive to the agencies' CIOs as what they thought were those projects most in need. Digital signature was one; FirstGov is another that I can think of off the top of my head.

This year we took that same fund—\$7 million is not a very large amount considering that we spend billions in other areas—we increased it to \$17 million. All indications are the Treasury-Postal will increase it. That should be significantly enhanced because there are opportunities. But what we have done again for the 2001 budget for the \$17 million was to go back to the CIO Council and the CFO Council and say, what is it that you think is most desirable, and this is reviewed within OMB. And they came up with these different types of projects that they wanted us to fund.

Mr. TURNER. Is that the only cross-agency initiative that OMB has been involved in?

Ms. KATZEN. No. Clinger-Cohen also includes a "pass the hat" authority. And there was an additional \$5 or \$6 million that we used to collect additional moneys from the various agencies for some of the CIO-type functions. Again, Mr. Flyzik, who helped implement this, could give you more details on it. But that's another opportunity.

And the third opportunity is there could be a lead agency. For example, on FirstGov, even though we're using some of the inter-agency money, GSA is the lead agency and is, in effect, sponsoring this, and they have the resources that we have reprogrammed to make sure that they can carry this out. There are other instances where other departments—Treasury, the Treasury Department is working on digital signatures. We have a \$7 million request, which unfortunately does not look like it's going to be funded. We could

use your help there. But that would be where they're taking the lead for the government. And I think that's correct, if I'm not mistaken. But they're the lead.

So in different areas we'll ask different departments to be a lead agency. So that, pass the hat and the interagency fund, all get worked together. We use as much creativity as we can because the technology is developing an awful lot faster than the budget process, and you come up with new ideas in the middle of cycle, you want to fund them. You want to figure out how to do it lawfully.

Mr. TURNER. I think that pass the hat problem, we discussed that at the hearing yesterday, is one of the problems that we see in our present pursuit of information technology.

Ms. KATZEN. It has drawbacks.

Mr. HORN. We will have another round here.

The gentleman from Virginia, Mr. Davis, 5 minutes. It's your turn.

Mr. DAVIS. Just a couple of questions.

You addressed the establishment of the Y2K Council with John Koskinen, who did an outstanding job, I think we can all agree, as chairman. It's unclear to me how the need to establish a Y2K Council in 1998 validates OMB's role in managing information resources. It seems to me that instead it demonstrated OMB's inability to gather the necessary expertise and foresee the need to address the Y2K problem in a more timely manner and its subsequent inability to manage governmentwide Y2K remediation without bringing in someone like John Koskinen to head the whole thing up and to have the clout, and that you don't want to keep doing this kind of thing. Could you give me your comments on that?

Ms. KATZEN. Well, Mr. Davis, OMB had been responsible for the governmentwide Y2K efforts, and, in fact, as Administrator of OIRA, it was one of my primary responsibilities, and we set in motion the processes that the Federal agencies would use. We established the reporting practices. We established the CIO Council's involvement in this; the Y2K committee that I met with once a month, we did a lot of things within OMB. By 1998, it became clear that the issue was not just the Federal systems. The issue was the country. And there was banking and finance, there was energy, and it was more than the country. It was international as well.

And so we discussed within the administration bringing in somebody who would focus attention, who would capture people's imagination, and who would work with State and local governments. I had already been meeting with NASIRE people in 1995, 1996 and 1997. John Koskinen took it over. He worked with State and locals. He worked with the private sector. He worked with the international Y2K effort.

The responsibility for the Federal systems themselves remained at OMB. We were the ones who did the quarterly reports. We were the ones who met with the laggards or those who were not moving as quickly as they should have. We were the ones who went to the President or the Vice President when we wanted additional help. John Koskinen was superb, and he was a superb candidate for this because he had just stepped down as DDM at OMB, and he knew where all the levers were. He never wanted to take from OMB its

authority, but he wanted to work with us, and that was a very good mix.

I was made the vice chair of the Y2K Council to keep the OMB piece of it intact. And I heard Mr. Doll say that Mr. Koskinen is a great model, and then he used the term "for a single project." I agree with that. I think if there's a single project that you want done sometimes, you find somebody who has the stature, the experience and the connections to do it. But if you're talking about something like all of information technology, Mr. Doll also said you can't separate technology from government programs. That's the whole thing. Then I am less amenable.

Mr. DAVIS. I want to get you out of here. I just look at it differently. You did a great job, but you had so many other things to do over there at OMB. You just did. You have so many responsibilities. You performed them admirably. I've worked with you on a lot of issues, and you're a great civil servant. But the problem was in that particular case you had too many things. The same thing concerns me with OMB and its structure today in giving it the emphasis. So I just look at it a little differently.

But I'm really interested to hear your perspective. I appreciate your sharing it with me. I may get back to you with a couple of other questions just for the record so we can fill this up.

You made one other comment that the administration will be changing, and at least we will have a new President and probably some new people, and we don't want to act precipitously. I agree. I'm just putting down a marker to say this is my concept, and we want to solicit advice on this as we move forward. This is kind of a work in progress. But I just wanted to share my thoughts, and I appreciate hearing yours. Thanks.

Ms. KATZEN. That's very helpful. Thank you, sir.

Mr. HORN. Does the gentleman yield?

Mr. DAVIS. I yield back.

Mr. HORN. The gentleman from Texas Mr. Turner. I'll give you 4 minutes this time because I want the last 3 minutes.

Mr. TURNER. Thank you, Mr. Chairman.

I concur with what my friend Mr. Davis said. I think we are introducing these bills here in the latter month of this Congress in order to get the issue on the table and begin to discuss what kind of structure a Federal CIO should have, because we know whoever is President is going to make this a part of their new administration.

And I want to say that, you know, GAO made the comment that the benefit of a Federal CIO is the ability to focus exclusively on information technology.

Your training is an attorney, as is mine. You practice regulatory and administrative law. You wear a lot of hats. You're the head of the CFO Council, the CIO Council, the Procurement Council. Even your Deputy, Mr. Spotila, who is the head of the Office of Information and Regulatory Affairs, has a wide range of duties, one of which is information technology, but he is neck deep into regulatory affairs in his office. And I think what we are trying to do here is to pursue a new position that has the exclusive ability to focus on information technology across government; to put in that position an individual who has the background, the experience and

the educational training to suit he or she to the position of a chief information officer as we find in the private sector. And I think that by doing that, we will see more opportunities for cross-agency cooperation, and we'll see the Federal Government move forward at a much more rapid pace than we've seen in the past.

That is not to say we are critical of anything you have attempted to do, but I think the emphasis on information technology is long overdue. And I know that you want to work closely with us to be sure that if we implement a Federal CIO, that it integrates well with your traditional functions. And I know that is one of your priorities, and we want to work with you in that regard.

Ms. KATZEN. Exactly. I appreciate that because I think there is much merit to this call for higher visibility, more focus or single-mindedness as it were. And my concern is that it be fully integrated within OMB because they have the budgeting and the management function governmentwide, and you can't easily separate the two. But the repeated calls for higher visibility and more single-mindedness, I think, have tremendous merit, and I appreciate your comments in that regard.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. I thank the gentleman.

My question is this: I appreciate you giving us the history there, and that's some of it we learned new. But the fact was that nothing happened after this committee started the movement in April 1996. We wrote the President with the ranking Democrats at that time writing with us on the letter to put one person in charge in the executive branch. That was July 1997, and he finally got around to it in late 1997 and 1998 when Mr. Koskinen was brought out of retirement. While he was there in your position, he really didn't do anything on this. You were doing the work there, as I remember.

Ms. KATZEN. I was doing that, yes.

Mr. HORN. And then he retired—

Ms. KATZEN. Although I reported to Mr. Koskinen, and he was aware of what I was doing, and he had sufficient confidence in me that he let me continue doing it.

Mr. HORN. Well—

Ms. KATZEN. And I had sufficient confidence in him that when we talked to the President and said, I think we ought to find somebody, he was the first person that came to our mind, and we called him. He was only in retirement for 2 weeks before we got him back.

Mr. HORN. He was in retirement, and he did not come back on board until April 1998.

Ms. KATZEN. Correct.

Mr. HORN. He was on a honeymoon with his wife. So the fact is during this time, FAA, the IRS, billions of dollars were going through those things. Now, did your group at OMB pull the plug? Why not when you have that many billion dollars going right down the drain?

Ms. KATZEN. We did, in fact, review the FAA information systems—we're not talking Y2K now. We're talking the information systems themselves—the FAA system, the IRS system, which Mr. Flyzik can talk about the history of that through this past decade, the HTM system. There was a health system at HCFA.

Mr. HORN. Right. They spent a few billion, too.

Ms. KATZEN. It was unbelievable. It was custom-built.

As I said in my testimony, when we came into office, there was an established pattern. Federal systems were to be custom-built with all the bells and whistles. They would inevitably come in over budget and so late that they would be obsolete by the time they were fully implemented.

We changed that. We changed that with your help. We changed that with the help of Raines' Rules. We changed that. We're now focussing on open architectures, modular development. The whole Raines' Rules capital planning concept has turned it around, and you don't have those kind of unfortunate headlines as frequently by a long shot at the end of the decade that you did at the beginning of the decade. It took us time to turn it around. That was what I was focusing on at the beginning part of the century—decade.

Mr. HORN. Who pulled the plug, OMB or the agency? Did the agency finally think about it, that they weren't managing anything?

Ms. KATZEN. We worked together. We're collegial. We raised issues—

Mr. HORN. I know. Collegially with the taxpayers' money to the tune of \$7 billion.

Ms. KATZEN. Well—

Mr. HORN. That bothers me. The fact is nobody made the tough decisions except Raines. I thought Raines really knew what he was doing when he came in there. And we worked together on the questionnaire and all the rest of it. He was a very right-on-the-spot person. He might have pulled the plug. I don't know.

Ms. KATZEN. The health one was ended before Mr. Raines became the Director. It was while Ms. Rivlin was still the Director of OMB that we stopped the health one. We stopped them when it became clear to us that this was not the way to go, and we worked with them. They're individual cases. Individual systems presented different problems within the agencies because they had different needs. FAA's need was that they couldn't be without a system because of the security of the air traffic controls. We had to make sure that whatever we had was enough to bridge or link, and so it was not just possible to say, well, let's stop that and forget all about it and go to someplace else. We had to work to a transition. The IRS is one that took a different turn that Mr. Flyzik can talk to.

Mr. HORN. Let me ask my last question. I know you have to go.

Yesterday the subcommittee released its computer security report card for the Federal Government, with the government receiving a D minus overall. Given the Office of Management and Budget's oversight responsibility for agency computer security programs, how do you explain this?

Ms. KATZEN. Well, Mr. Chairman, I think, as Mr. Spotila indicated yesterday, we do not completely agree with the grades.

Mr. HORN. Not one person under oath in this room disagreed with any grade. And if they're doing that to the press, they didn't do it here.

Ms. KATZEN. I was not here yesterday. Mr. Spotila was testifying. My understanding is that a lot of the agencies—departments

were, as they should be, totally candid about we're doing partly here, we're not doing anything here, we're doing something here. In some of the grades they got no credit for any of the things that they were doing.

Grades come as a snapshot in time, and unlike the Y2K where you have a single function that you want to sort of track over time, and you can see whether you're 68 percent remediated, 98 percent remediated, you get all the way to 100 percent, with security there are a variety of different measures and a variety of different standards depending upon the sensitivity of the information, because your security should be commensurate with the risk of loss. And a DOD is a very different animal from the Department of Agriculture, for example, where a civilian agency does not have to reach the same standards.

Having said all of that, I would remind you that when Mr. Koskinen came into the office, the government was given a D minus also——

Mr. HORN. That's right.

Ms. KATZEN [continuing]. For Y2K.

Mr. HORN. And he got it up to a B, which is great.

Ms. KATZEN. What happened was in the 2-year period, because of the foundations that we had laid and the work that had been done by the Federal employees, there were no disasters at the date change. The Federal systems held together magnificently. People were ready ahead of time. And if we get a B minus when we actually end up having a nonevent, there's some sense that maybe the grading on the curve could be a little bit adjusted.

Mr. HORN. It isn't graded on the curve. It's graded on the absolute. And remember that this is self-graded by the agency, not us.

Ms. KATZEN. They didn't give themselves a D minus. You took the information and gave them the grades. They didn't give themselves a grade. If you ask the agencies, and Treasury is here today, whether they deserved the grade they got or whether they thought that their work in process is warranting some other grade, I would be very interested in the responses, because what I hear is that they feel that the grading was kind of tough.

Now, I did well in school with professors who gave tough marks, and I like to rise to the occasion, and I like to fight back, and I like to say, OK, you give me a B, I'll show you. I'll get my A.

Mr. HORN. Good. We're glad we stimulated OMB to do something. And if it takes that, why we'll give them a D minus or a D plus next time.

But, no, what we want is something that solves this, and we want people that make tough decisions with the taxpayers' money. That's what I'm concerned about. That's what every Member here regardless of party is concerned about. We can't afford these \$4 billion boondoggles.

Ms. KATZEN. I share your—I agree with you completely.

Mr. HORN. With security they can do a lot of things. They just haven't because there hasn't been the focus.

Ms. KATZEN. Well, and we haven't gotten the funding.

Mr. HORN. They always say that. All you do is pull the plug on a few things. Energy is the prime example.

Ms. KATZEN. No, I'm sorry. What I meant—you may have misunderstood what I was staying. We have repeatedly requested the Congress to fund in the security area for FIDNA, for FEDCERT, for Cyber Core. There was a \$90 million critical information protection piece that the Congress has not funded.

We have requested funding for security again and again, and over the last several years and even right now the IRS piece is not fully funded. Apart from the security is the modernization that they need to do.

So it's not that we're holding back, but I share your objective which is not to waste taxpayers' money, which is to provide the best service possible, to do it in a way that is reasonable and rational and responsive to the American people.

I agree completely with where you're coming from, and, again, as I said in my opening statement, we think that the work that this committee has done has been very important and instrumental in helping us with whatever progress we have achieved, and we thank you for that.

Mr. HORN. Let me ask the last question. Do any of the people here, and that includes the people who haven't had a chance to make their presentations, do you have any questions of the administration before Ms. Katzen leaves? Anybody want to raise their hand or something? Any question you've been wanting to ask the administration but couldn't? OK. Forever hold your peace, or talk to them on the side.

Ms. KATZEN. Thank you, sir.

Mr. HORN. We thank you for staying, and we hope we haven't delayed you, but we're within 6 minutes. Thank you.

We now go back to the presenters. Next is Paul E. Rummell, president and chief executive officer of RLG netPerformance, Inc., former Chief Information Officer for the Government of Canada.

We're delighted to have you here, and we want to get a lot of your experience on the record.

STATEMENT OF PAUL E. RUMMELL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, RLG NETPERFORMANCE INC., FORMER CHIEF INFORMATION OFFICER FOR THE GOVERNMENT OF CANADA

Mr. RUMMELL. Mr. Chairman, Mr. Turner, Mr. Davis, members of the subcommittee and distinguished panelists. I am very pleased to speak with you regarding establishing a Federal Chief Information Officer position in the U.S. Government. I have a unique perspective to share with you. I served as the first CIO for the Government of Canada, and I am an American citizen and a Canadian citizen. I have 28 years' experience in information technology.

The role and mandate for Canada's CIO position is to bridge the direction and evolution of technology in government; work to improve relations with the vendor community; renew the IT community within the government, and tackle the inertia in Treasury Board and across the government by resolving key concerns effectively, like privacy and security.

I reported to the Secretary of the Treasury Board and had a liaison and strong communication with the Prime Minister's office. My responsibilities were a \$3-billion-a-year budget, 16,000 employees,

and a portfolio of 80 some departments and agencies, and I had a mandate to eradicate the year 2000 bug.

Policy and management were focused on larger departments like Public Works, Revenue Canada, National Defense, Human Resource Development Canada, Industry Canada and the Department of Justice. Twenty of the largest departments and agencies were represented in a core committee which I chaired, and I consulted with smaller agencies and departments less frequently.

I established a Council of Provincial CIO's to coordinate activities between their jurisdictions, and we met with other levels of government to coordinate service delivery initiatives for our government.

The CIO position has made an impact on Canada's Federal Government success in information technology. We moved beyond establishing policy to a strategic leadership role with operational focus and delivered results in three key areas: infrastructure, innovation and service to the IT community.

Infrastructure is the platform used to deliver cost-effective, unified services to citizens. It's not just wires and networks, but INFOstructure, the policies, standards, procedures and directions that make interoperability a reality. It is the combination of people, process and technology to capture the imagination and achieve results.

As CIO and an information exchange specialist, I was and continue to be in the business of innovation. The approach must be to balance risk and fiscal responsibility. The CIO position should be in a place that empowers solutions, from structural changes and alternate service delivery models to partnerships with other governments and the private sector.

The CIO's core mandate was to provide advice, expertise and service to the information community across government, and my goal was not to get in your way, but to get things out of your way.

We managed technology spending envelopes to be sure that we were making appropriate investments. We helped get the government through some challenges with megaprojects. We worked with the vendor and outsourcer communities to ensure modern procurement and project management procedures were in place.

Information technology provides one of the cornerstones for the renewal of government. It is essential that the U.S. Government adopt a modern organizational structure with a Federal CIO to lead, make a real difference and encourage cooperation.

It is your challenge as a subcommittee and as a government to play a leadership role in establishing a position that will direct the appropriate use of technology in our government. Based upon my experience, I favor the recommendation that the Federal CIO report to the Office of the President. I believe the position will be most effective in this structure.

To sum up, these are exciting times. The new Federal CIO for the U.S. Government will have an ambitious agenda in this year 2000 and beyond. Effective use of technology will enable us to work harder, faster and smarter. This is not an end in itself. What counts is what it will enable us to do, and that is to serve Americans better. Thank you.

Mr. HORN. Well, we thank you. Those insights are very helpful. [The prepared statement of Mr. Rummell follows:]

***“Perspectives on Establishing a
Chief Information Officer Position
for the US Federal Government”***

**Notes for remarks by Paul E. Rummell
President and Chief Executive Officer of
RLG netPerformance Inc.
Former-CIO for the Government of Canada**

**To the Congress of the United States
House of Representatives
Committee on Government Reform
Sub-Committee on Government Management,
Information and Technology**

September 12, 2000

BACKGROUND

Technology exerts a profound influence on the everyday lives of Americans and Canadians. The use of IT is growing by 15-20% a year, compounded annually, and there are 10,000 new Web sites every day. The amount of information being maintained on the Internet is skyrocketing - what we have seen is not just change, but a revolution!

This poses some complex challenges as governments re-examine the way they manage and operate. Americans have high expectations of their government; if they can't do it well, they shouldn't do it at all. To meet public expectation, it is essential to improve service delivery using technology in new ways.

Powerful new technologies are becoming the infrastructure for the 21st century; our society is based on the exchange of ideas, information, knowledge and intelligence. Governments are digitizing information, working together to share information in ways inconceivable a decade ago.

The day is at hand when a citizen picks up the phone, dials one government number, gets the information he/she needs, registers the information and receives the results instantly in a secure, electronic environment. This is end-to-end electronic service. It is the ultimate example of what government can do for its citizens.

The convergence of people, process and technology is key to any IT solution. Implementation of information systems is 50% management, 35% marketing, but only 15% technology. The 85% has historically not had enough focus, and that is where the challenge lies.

CHECK AGAINST DELIVERY

Mr. Chairman, Members of the Sub-Committee on Government Management, Information and Technology - I am very pleased to speak with you regarding establishing a Federal Chief Information Officer (CIO) position in the US Government.

INTRODUCTION

I have a unique perspective and experience to share with you regarding this position. I served as the first CIO for the Government of Canada and am both a US and Canadian Citizen. I have 28 years experience in information technology, including partnership in a big-five management consultancy, and various executive positions in private and public sectors.

The role and mandate for Canada's CIO is to:

- Bridge the direction and evolution of technology in government;
- Work to improve relations with the vendor community;
- Renew the IT community in government; and
- Tackle the inertia at Treasury Board and across government by resolving key concerns like privacy and security.

I am confident that the CIO team, under my direction, was effective in moving this agenda forward for the Government of Canada.

THE CANADIAN CIO

First, let me explain the structure of the Canadian CIO position, and then I will provide examples of some strategic initiatives we were able to accomplish.

I reported to the Secretary of the Treasury Board and maintained a liaison with the Prime Minister's Office. My responsibilities encompassed a \$3 billion budget, 16,000 employees, and a portfolio of 80+ Federal Departments and Agencies. I had an immediate mandate to coordinate the effort required to eradicate and remedy the "year 2000 bug" in thousands of systems.

Policy and management were focused mainly on larger Departments like Public Works, Revenue Canada, National Defense, Human Resource Development Canada, Industry Canada, and the Department of Justice. A Core Committee included 20 of the largest Departments and Agencies, with smaller groups consulted less frequently. I established a Council of Provincial CIO's to coordinate inter-jurisdictional activities, and met with Federal, Provincial, and Municipal CIO's as needed to discuss integrated service delivery opportunities.

WHAT WE ACCOMPLISHED

Creation of the CIO position made a significant impact on the Federal Government's success in the information technology arena. We moved beyond policy to a strategic leadership role with an operational focus, and delivered results in three key areas:

- Infrastructure;
- Innovation; and
- Service to the IT community.

Infrastructure

Infrastructure is the platform used to deliver cost-effective, unified services to citizens. Without infrastructure, we cannot deliver end-to-end electronic transactions, share information, or work in concert across agencies, departments, and other jurisdictions. It's not just wires and networks, but **info**structure; the policies, standards, procedures and directions that make inter-operability a reality. It is the combination of people, process and technology that drives the vision. The vision for government has to capture the imagination, yet it must be achievable in the near term in a step-by-step way.

Under infrastructure, we identified four areas for action:

- Access and security;
- People;
- Horizontal governing; and
- Policies.

Access and security

Citizens want instant access, informed answers and fast service. They want a single window into government. They need to access a wide variety of information with assurances that their privacy will be safeguarded.

Security is one of the biggest challenges we face as we move towards electronic service delivery. The infrastructure required to allow secure messaging and transactions is central to maintaining the trust of all citizens.

People

The IT community includes the people in our government who make the country, government programs and services run, and serve as a cornerstone for future service delivery.

The need for up-to-date IT skills is greater now than ever before, and both public and private sector organizations around the world are competing for the same scarce pool of skilled resources.

Attracting experienced, more senior people and retaining existing employees are challenges all IT organizations are facing. Another common concern is raiding – many employees hear the siren call of higher wages and better perks. We worked with many HR communities to develop innovative solutions; exploring partnership arrangements with industry, providing attractive compensation and benefits packages, offering incentives such as flexible work hours, training programs and opportunities for career

fast-tracking, creating a vital learning culture and continued role for IT expertise in government.

Horizontal Governing

Traditionally information systems have evolved vertically – each agency and department, each level of government building their own “silos” or stovepipes of information. This was acceptable before networking and the Internet.

We worked across departments through a Shared Systems Initiative to reduce the number of discreet administrative systems from over 120 to about 14. We built and maximized horizontal linkages and bridges between information systems. For example, the Department of Justice lawyers in all departments access information at a ‘home base’; the Integrated Canadian Health Network provides linkages between Federal & Provincial Governments and local communities - one coherent solution for our common client, the taxpayer and citizen.

The growth of horizontal governments means that old reporting mechanisms no longer address the new realities. The Federal CIO must accelerate the dialogue with agencies and departments to build a common IT and information management infrastructure.

Policy

The CIO’s office was responsible for: information security, secrecy, privacy, access to information, appropriate use of the Internet, federal identity, information retention, records, information management and standards to technology integration. Establishing and maintaining these policies was a huge effort, but central coordination has provided real efficiencies.

Innovation

As CIO and an information worker, I had to be in the business of innovation. The style of innovation can’t be compared to that of a high-flying Silicon Valley entrepreneur. There should be no precarious leap of faith in this process; the approach must be to balance risk and fiscal responsibility. The CIO position should be established in a place that empowers a spectrum of solutions from structural changes and alternate service delivery models to partnerships with other governments and the private sector.

Service to the IT Community

The core of the CIO mandate was to provide advice, expertise and service to the information technology and information management communities across government. I was meant not to ‘get in your way’, but to ‘get things out of the way’.

We were able to provide for effective, early recognition and resolution of the year 2000 date challenge in all levels of government. I also worked with senior people from some of the largest organizations in Canada to establish an effective approach to dealing with this issue in industry and small-to-medium sized enterprises.

We reviewed Federal technology spending envelopes to be sure we were making appropriate investments. We managed mega projects, which have plagued many government agencies and departments, and helped to get the government through some challenges in this area. We worked with the vendor and outsourcer communities to ensure we had modern procurement and project management procedures in place.

SUMMARY

Information technology provides one of the cornerstones for the renewal of government, creating a tremendous acceleration of the US economy. It is essential that the US Government adopt a modern organizational structure with a Federal CIO who has the ability to lead, make a real difference and encourage cooperation. This role must provide for effective rationalization and coordination of the United States Government's tremendous technology and information resources.

The function of the Federal CIO will be to ensure that there is delivery of effective and efficient government services throughout the US and to others that depend on the leadership role of the United States. We cannot innovate if the same obstacles keep reappearing in our radar. We cannot learn from the vast expertise we have in our government if we do not share the information we have available to us. The Government's challenges are similar to those faced by other major organizations around the world.

It is your challenge as a Sub-Committee to play a leadership role in establishing a position that will direct the appropriate use of technology in our government. I applaud the initiative of the two Congressmen that have put bills forward supporting this move. *Based upon my experience – being there - I favor the recommendation that the Federal CIO report to the Office of the President rather than to the Office of Management and Budget.*

I believe the position will be most effective in this structure. I know the efforts for successfully resolving the year 2000 challenge were particularly effective from this special reporting relationship to the President in the Executive Branch.

These are exciting times. The new Federal CIO for the US government will have an ambitious agenda. In this, the year 2000 – and beyond, effective use of technology will enable us to work harder, faster, and smarter. It is not an end in itself. What counts is what it will enable us to do, and that is to serve Americans better.

Thank you,

Mr. HORN. Our next presenter is Robert D. Atkinson, director of technology & new economy project for the Progressive Policy Institute.

Mr. Atkinson.

STATEMENT OF ROBERT D. ATKINSON, DIRECTOR, TECHNOLOGY & NEW ECONOMY PROJECT, PROGRESSIVE POLICY INSTITUTE

Mr. ATKINSON. Thank you, Mr. Chairman, Mr. Turner, Mr. Davis.

I was the author of a report that PPI released a few months ago called "Digital Government, The Next Step to Reengineering the Federal Government." In that report we concluded that the single most important thing the Federal Government could do to foster the speedy transition to a digital Federal Government would be for Congress to create the position of a Federal CIO. Therefore, I strongly support the committee's efforts to do this as embodied in H.R. 4670 and 5024.

Mr. McClure mentioned in his testimony that when Clinger-Cohen was passed in 1995, that there was a debate whether we should create a Federal CIO at that time, and the decision was no. That may have been a reasonable decision at that time. I'm not sure. I wasn't involved in it then. But it's not now, and the reason for that is there's a saying in the Internet community that the Web changes everything. And I think the Web does change everything in government. And now for the first time—we could not just talk about the notion of functionally oriented government and moving beyond the stovepipes that Mr. Flyzik talked about, but we can do it now for the first time.

We have the technology that lets us think about creating customer-oriented government. To do that, though, we need a management system that moves beyond just single agencies, thinking about an IT research from an agency's perspective. And I would argue we need to think about it on two levels. One, as I mentioned, is a functional-based, not agency-based, government. And there are a host of applications that one can imagine. One place for people who are engaged in exporting and importing. In fact, there's a program I will mention, the International Trade Data system. One place for companies to come and find out all the regulations that they have to deal with. One place to find out about education and training resources. One place to find out about health. All of these things can be done on a functional basis.

Second, we need to think about an enterprisewide information architecture. There are a whole host of issues with regard to issues of data sharing, data collection, new types of interactive tools, expert systems, information on request systems, data base systems, and other wide-ranging issues which you've mentioned, security, privacy, digital signatures. All of those issues are essentially best handled on an enterprisewide, Federalwide level.

Well, I think you've heard some arguments as to why the existing organizational and management system can do this. I would argue that the existing organizational system is really a function of the old legacy system, the old agency-by-agency system, and it

isn't suited to doing what we need today. Obviously the proof is in the pudding.

Let me mention two things. I don't really see a Federal digital government conversion plan right now. I don't think there is one. I haven't seen it. I think we need to have one to manage the overall resources.

Second, let me mention one example of, to me, a very strong effort to do digital government on a functional basis, the International Trade Data system. ITDS was a great idea. It was developed—to take 104 different Federal agencies' programs or bureaus and streamline the collection and reporting of trade data. That system is essentially still in the water. It's not moving anywhere, and Customs has really taken over the charge and is planning to build a proprietary system. And we don't need a proprietary system. What we need is a functional system.

And I would argue that if we had a CIO, the CIO's leadership would have been critical in making the ITDS system come about.

There's another criticism that the CIO would add a layer of bureaucracy and delay, and that we don't need it because we already have that management system. I think it's interesting, we have 20 States now, or more than 20 States, that have cabinet-level CIOs that report directly to the Governor. In each of those 20 States, they also have their respective OMBs. They have Departments of Administration. They haven't eliminated those Departments of Administration. But what those Governors in the 20 States have realized is that digital government is so important to the functioning, to the mission of the Governor, of their administration that they need to create somebody whose mission it is to solely do that.

And I think, Mr. Chairman, you've made that point, that it's not really a question of OMB falling down on the job. It's just that it's not their core mission. We need some institutions where that is the core mission.

Last, there is a notion, well, maybe we don't need this because we can do this as single projects. And, again, the notion of Mr. Koskinen and the Y2K czar—and I'll quote Ms. Katzen saying that what was key about Mr. Koskinen was that "focused attention, captured imagination, and worked with State and local governments and the private sector."

To me, that's what we need to be doing every day. It's not just a Y2K problem. It's a security issue. It's a privacy issue. It's reinventing our Federal Government. We need somebody who does that as their mission on a daily basis.

Let me close by saying this really isn't something that—I think you heard from Mr. Doll that States are doing this. The private sector is doing this. The old model in the private sector was that the person in charge of information technology was down in the bowels of the company buying computers and servicing them and that sort of thing.

The new model is that companies are creating CIOs that report directly to the CEO and are partners with the CEO. Let me quote Cisco CEO John Chambers. He recently stated, "the role of the top information executive has been elevated to that of a strategic partner with the CEO and the CFO." Corporations are doing that for a reason because they realize that without transforming their own

companies into digital companies, they're going to be left behind in the marketplace. I would argue it's time we need to do that for the Federal Government.

Thank you very much.

Mr. HORN. Well, thank you.

How long is that report that you mentioned?

Mr. ATKINSON. The report that we issued, very readable, is about 13, 14 pages.

Mr. HORN. OK. I would like to put it in the record at this point if I might.

Mr. ATKINSON. I will submit it.

Mr. HORN. Thank you very much.

[The information referred to follows:]



Digital Government

The Next Step to Reengineering the Federal Government

Progressive Policy Institute
Technology & New Economy Project

Robert D. Atkinson and Jacob Ulevich

March 2000

About the Progressive Policy Institute

*"One person with a belief is a social power
equal to ninety-nine who have only interests."*

—John Stuart Mill

The mission of the Progressive Policy Institute is to define and promote a new progressive politics for America in the 21st century. Through its research, policies, and perspectives, the Institute is fashioning a new governing philosophy and an agenda for public innovation geared to the Information Age.

This mission arises from the belief that America is ill-served by an obsolete left-right debate that is out of step with the powerful forces re-shaping our society and economy. The Institute advocates a philosophy that adapts the progressive tradition in American politics to the realities of the Information Age and points to a "third way" beyond the liberal impulse to defend the bureaucratic status quo and the conservative bid to simply dismantle government. The Institute envisions government as society's servant, not its master—as a catalyst for a broader civic enterprise controlled by and responsive to the needs of citizens and the communities where they live and work.

The Institute's work rests on three ideals: equal opportunity, mutual responsibility, and self-governing citizens and communities. Building on these cornerstone principles, our work advances five key strategies to equip Americans to confront the challenges of the Information Age:

*Restoring the American Dream by accelerating economic growth,
expanding opportunity, and enhancing security.*

*Reconstructing our social order by strengthening families,
attacking crime, and empowering the urban poor.*

*Renewing our democracy by challenging the special interests and
returning power to citizens and local institutions.*

*Defending our common civic ground by affirming the spirit of
tolerance and the shared principles that unite us as Americans.*

*Confronting global disorder by building enduring new international
structures of economic and political freedom.*

The Progressive Policy Institute is a project of the Progressive Foundation. For further information about the Institute or to order publications, please call or write:

600 Pennsylvania Ave., SE · Suite 400 · Washington, DC 20003
E-mail: ppiinfo@dlcppi.org · WWW: <http://www.dlcppi.org>
Phone (202) 547-0001 · Fax (202) 544-5014

Introduction

"I have in general no very exalted opinion of the virtue of paper government."
Edmund Burke

Imagine a future in which citizens can log onto one Internet site, easily find the government services they are looking for, and use that site to conduct an online transaction; a future in which businesses fill out one Internet form for all their local, state, and federal environmental regulatory compliance requirements; a future in which government officials make all purchases and payments electronically, saving millions of dollars. The technology for all these applications and others is here today, waiting to be adopted by the federal government.

Indeed, these technologies are rapidly spreading in the commercial sector. The economy is evolving to the point where a significant share of economic transactions will soon be conducted through electronic means. Digital technologies are fundamentally transforming our economy and society, and have the potential to transform government. In fact, a key next step in reinventing government involves the widespread application of information and communications technology to the delivery of government services—in short, fostering digital government.

Among the potential benefits of digital government are savings in money and time for the government, consumers, and businesses. If banks can cut their transaction costs by 90 percent through online banking, similar savings for gov-

ernment are likely.¹ Moreover, users of government services will benefit by greater access to higher quality services. Most importantly, the relationship between government and citizens can evolve from its traditional hierarchical and arms-length one to a more reciprocal one where citizens are genuine stakeholders in their government.

Done right, digital government promises to transform Industrial Age big government into Knowledge Age smart government. Old economy government was organized around agencies and bureaucracies that operated like "stove pipes" with little information flowing between them, and with operations developed to meet the requirements of agencies, not the needs of citizens. New Economy government will be organized around the functions and the needs of citizens; with information and communication technologies a key enabler of this reinvented government.

Moving to digital government will speed the transition to a digital economy. Part of why this transition is not proceeding even faster is because of "chicken or egg" issues. For example, smart cards have diffused slowly through society, in large part because consumer value is limited as long as few merchants accept them, and few merchants accept them as long as few consumers have them. Similar issues exist with regard to digital authentication, educational software, and to some

Digital Government

extent the Internet itself.² These impasses will be broken, but if the federal government became a leading-edge, or even “middle-edge,” user of information technology (IT), it would enhance the value of being online and speed the transition.

Despite the obvious promise of digital government, it has not yet become a priority of most policy makers. Congressional committees have largely ignored the issue. And while the Administration has articulated goals and begun projects, much more can be done. In the meantime, the issue has remained the province of technologists focused on technically complex issues not readily understandable to policy makers, much less to citizens in general.

In part because of this technocratic focus, digital government progress to date has been slow and not linked to government reinvention. Rather, most IT applications have focused on improving

the efficiency of existing operations or providing one-way information dissemination, instead of on fundamentally changing the way businesses and citizens interact with government. As a result, another kind of digital divide is emerging—between government, which is only moving tentatively into digital operations, and the commercial sector, which is moving at “web-speed” into e-commerce.

This report lays out the overall direction the federal government should take to foster digital government and describes how the government can use IT to transform its operations. It first discusses the factors that have slowed progress to date and then describes 12 key principles to follow in implementing digital government. It then lists four major policy recommendations for implementing digital government. Finally, it examines what government is doing now and what it should be doing.

Impediments to Faster Progress Toward Digital Government

At the federal level, considerable progress has been made toward establishing a vision for digital government and providing information to the public through agency web sites. But, relative to the capabilities of the technology, much more can be done. There are at least four factors that have hindered progress: 1) lack of top-level agency and government-wide leadership; 2) lack of funding and flexibility to implement digital government projects; 3) the prevalence of a traditional “agency-centric” government paradigm, rather than a customer-centric one; and 4) lack of pressure for change.

A Lack of Political Support for Digital Government

Congress and the Administration have issued broad and generalized mandates regarding digital government. However, congressional committees have largely ignored the issue. While the Administration has articulated progressive goals and begun projects—including innovative efforts from the Vice-Presidents’ National Performance Review dating back as far as 1995—more can be done. In fact, the NPR is a center for creative thinking on these issues, but their initiatives have not always received the high-level support needed to translate them into results. Cabinet secretaries in particular have generally not made digitizing government a top priority and see it as separate from their core mission (for an exception, see Box A, p.4). Nor has OMB been a strong advocate of digital government. Within agencies, Chief Information Officers (CIOs) normally do

have the authority and budget to implement significant digital government applications.

However, there are signs that digital government is receiving increased attention, both in Congress and the Administration. President Clinton issued an executive memorandum on the subject in December 1999, and the President’s Management Council has adopted the issue of digital government as one of their three top priorities for 2000. And in Congress, Senator Joseph Lieberman (D-CT), and ranking Democrat of the Senate Governmental Affairs Committee and Congressman Jim Turner (D-TX), ranking Democrat on the Government Management, Information, and Technology Sub-committee of the House Committee on Government Reform are both exploring the issue of electronic government with an eye toward introducing legislation this congressional session.

Notwithstanding recent efforts, it has up until now been hard to make needed progress, particularly to develop cross-agency applications. Currently, each federal agency has an individual information technology plan, usually created without regard to the need to develop cross-agency applications. Compatibility on a government-wide scale was not the original aim of government IT use and has resulted in a cacophony of systems—proprietary, and non-proprietary; and common and rarely used software and hardware.

While inter-agency IT compatibility issues are important, so is the incompatibility of systems within individual agencies. For example, some employees at the State Department have to use up to

BOX A: Success with Digital Government and the Federal Geographic Data Committee³

Anyone who has ever looked for anything on the Internet knows the frustration of trying to whittle down a search to get to the useful information. Now imagine searching the Net to find a particular map and its underlying data with the right scale and features for your application. Without a common means of describing geographic data, the search could be long and fruitless. Fortunately, an obscure federal interagency committee—aided by academics, states, businesses, and local government representatives—developed in 1994 a common way to describe geographic (sometimes called “spatial”) data like land elevation, population, vegetation, waterways, political boundaries, soils, and many other features. This “metadata standard”, recently revised, helps turn single-use data sets into widely used publicly available assets. It is an example of how government, working on the edge of technological development, can add significant value to private and other public sector investments in information.

Back in 1990, the Office of Management and Budget had the wisdom to establish the Federal Geographic Data Committee (FGDC) to oversee the coordinated development of common standards for map-making by 16 federal agencies like the Census Bureau, the U.S. Geological Survey, the Forest Service, the National Defense Mapping Agency, and the Transportation Department among others. As geographic information system (GIS) software developed in the early 1990s, FGDC focused its efforts on developing standards and protocols for just about every kind of data that could be represented on a map. While extraordinarily tedious to develop, these standards enable millions of users of geographic data to search and find information on the Internet, use data sets assembled by others, and make their own work widely accessible to others. A 1994 Clinton Executive Order further broadened FGDC’s mission and links to state, local, and tribal governments and the private sector under the banner of the National Spatial Data Infrastructure.

The Federal Geographic Data Committee is a story of how political leadership at the highest levels can transform an obscure bureaucratic backwater into a leading edge model of digital government. In 1993, soon after taking the helm of the Department of the Interior, Secretary Bruce Babbitt decided to become chair of the FGDC. (The previous chair had been the Deputy Director of the Geological Survey.) When he announced this decision at a senior staff meeting, he was greeted with hoots of laughter. Few of the political staff thought he was serious about delving into this most arcane—and boring—government activity.

In fact, Secretary Babbitt knew exactly what he was doing. He had seen with his own eyes during the negotiations on the Northwest Forest Plan in early 1993 that none of the dozen or so government agencies worked off the same map. Nor could the maps be made compatible with one another: land ownership boundaries didn’t match, and measures of scale and elevation were inconsistent, making a difficult policy and political issue even worse.

Secretary Babbitt understood the value of standard setting and coordination among federal agencies and their partners in state and local government. These partners, in fact, were often at the front line of tracking land use and fine-scale geographic features that can be so important in resource management. Because of the Secretary’s interest in the mission of the FGDC, all the other agencies had to revisit their representation on the Committee. By the next meeting, under secretaries and assistant secretaries were attending instead of GS-14 and GS-15 employees.

FGDC now directs a widely used, net-based clearinghouse of 188 spatial data servers, making access to geographic data possible in ways that text-based search engines could not. FGDC offers modest seed grants to states and local agencies to develop their own nodes for the NSDI. In addition, FGDC leads in the development of a nationally consistent “framework” data set, upon which virtually all map products in the future will be based. Finally, FGDC continually develops and revises the core data standards for making maps of population density, forests, soils, waterways, highways, biological resources, pollutant sources, and many other kinds of information that can be displayed on maps. With a modest budget of about \$3.4 million each year, FGDC more than pays its freight in adding value to hundreds of millions of public and private dollars invested in data gathering and map making.

The lessons for digital government from the FGDC are the following: involve cross-agency and intra governmental collaboration, focus on the end user customer, be web enabled, and drive it from the highest levels of political leadership.

three computer terminals to accomplish tasks, because of incompatible applications and systems.⁴

Concerted top-level leadership in both Congress and the Administration is necessary to harness contemporary technology to bring government into the 21st century. Leadership is also needed to foster inter-agency solutions. A number of committees and organizations work to foster government IT coordination. The National Partnership for Reinventing Government (NPR) has attempted to develop a number of cross-agency applications, and the Government Information Technology Services Board was created in 1993 to help implement NPR's recommendations. Similarly, the Chief Information Officer Council, made up of 54 CIOs or deputy CIOs from federal agencies, meet as an interagency forum to direct the implementation of federal IT resources. The Office of Intergovernmental Solution's Intergovernmental Advisory Board and the General Services Administration have also worked to develop innovative cross-governmental technology systems.⁵

But these interagency groups suffer from several distinct limitations. First, they lack the resources to implement government-wide efforts. Second, they are largely a meeting of equals, and lack the authority to impose central direction on individual agencies. Moreover, their primary focus remains on their individual agencies, not on government-wide reinvention. Third, without strong cabinet-level support, CIOs are limited in what they can get done, especially if it involves reengineering government. Fourth, because OMB itself is organized by stovepipe it has done little to promote cross-agency, enterprise-wide initiatives.

A final reason why elected and appointed officials have not done more to promote digital government until recently is because the private sector has done little to push for it. Unlike their support for important issues such as encryption export control reform, copyright protection, and digital signatures, business has been virtually silent when it comes to advocating digital government. Without the strong support of the technology business community, it is easy for policy makers to put this issue on the back burner, or to treat it simply as a narrow technical issue affecting government alone. The technology business community needs to educate Congress and the Administration as to why moving to a digital government is a critical step in the overall evolution to a fully networked, digital economy.

Lack of Funding and Flexibility

Government is being asked to manage paper and face-to-face government while at the same time creating a new digital government, but often without additional resources to do the job. While it is true that digital government saves money, there are short term costs for technology and project management. Moreover, agencies are limited by Congress and OMB in the amount of flexibility they have to reprogram funds toward digital government initiatives.

When funding is provided, it is usually to individual agencies. There is a conspicuous lack of funding for cross-agency applications and agencies are not apt to use their limited funds for them. Yet to effectively implement many digital government functions, government must take an enterprise-wide management perspective (whether it's delivering monetary benefits to the public, organizing cross-agency or individual agency databases, or developing government portals). This unwillingness to fund cross-agency projects is a principal reason why the development of the International Trade Data System has stalled, as the Customs Service has lobbied for funds for its own proprietary system (see Box B, p.6). Similarly, when the Small Business Administration sought to develop a single point of entry where small businesses who interact with numerous federal agencies could enter their data just once and have it shared with the various agencies, resistance by individual agencies scuttled the initiative.

An "Agency-centric" Rather Than a "Customer-centric" Paradigm Prevails

Government services are funded on an agency-by-agency basis. Congressional committee jurisdiction and OMB agency budget allocations sustain this stovepipe focus. Within Congress, committees and subcommittees focus on individual agencies, as does the oversight system. There are few means in Congress to take an enterprise-wide perspective.

However, the IT revolution provides the opportunity to reengineer government and to allow government services to be organized in ways that fit the needs of customers rather than the requirements of bureaucracies. Yet, because government officials usually view the world through an agency, or even bureau perspective, developing the will to create and implement digital government solutions organized around customers' needs has proven difficult.

As President Clinton stated in his recent memorandum on electronic commerce: "There has not been sufficient effort to provide government information by category of information and service—rather than by agency—in a way that meets people's needs."⁶ For example, many of the required forms for exporting can be downloaded from the Internet, printed, and mailed to the respective offices. While the online forms expedite the process considerably, it would be much more efficient if all of the pertinent information from various agencies were available in one form and automatically routed to the correct agencies at the push of the "submit" button.

This is not unique to the United States. A recent survey of UK citizens on digital government reported, "There is . . . a strong belief that [government] services have traditionally been developed from the producer rather than the user perspective and this has induced a feeling of powerlessness in dealing with government."

Just as the Internet threatens to disintermediate large sectors of our economy (for example, it has put out of business some brick and mortar retailers, middlemen, stockbrokers, etc.) it also threatens to disintermediate some government

functions. For instance, some in government have justified their positions by controlling and doling out information. Yet, by providing information freely on demand, digital government makes these functions obsolete. Only top-level leadership can overcome the resistance of government bureaucrats to potentially disruptive changes.

Lack of Competitive Pressures Forcing Change

Commercial e-commerce companies face enormous pressures to innovate, to be the first to commercialize applications, and to gain market share as rapidly as possible. As a result, in the frenetic Internet economy people talk about technological and commercial evolution in "Web years" (three months time) because the rules seem to change that often. In contrast, the federal government does not face these pressures, and because of this, has not operated with anywhere near the same speed and intensity as e-commerce companies. As a reflection of this, one federal official recently stated, in an informal context, that the federal government could afford to go slow because the Internet marketplace just wasn't big enough to justify an aggressive pace.

Box B: ITDS and the Challenge of Overcoming Stove-Pipe Government

In an effort to reinvent the system by which exporters and importers deal with regulations reporting requirements, the National Partnership for Reinventing Government proposed the creation of the International Trade Data System (ITDS). ITDS was intended to be a partnership of the Customs Service and a number of other regulatory agencies, including the Food and Drug Administration, the Environmental Protection Agency, and the Department of Agriculture, to accomplish a variety of trade-oriented tasks without the traditional hindrances of agency boundaries. The proposed system would allow importers and exporters to essentially fill out one master form that would combine all of the information all of the various agencies may need. This process would lead to cheaper, more accurate, and more timely exchange and recording of information, and expedite the physical movement of trade by reducing the time goods are kept at the border for inspection.

Yet, the ITDS story illustrates just how hard it is to develop true customer-centered government. From the beginnings of the process, the Customs Services viewed ITDS with suspicion. ITDS represents a cultural shift, one that would require Customs to share power and authority over trade with other agencies, something they are presently able to avoid. Because of this, Customs has resisted the development of a true interagency partnership. Customs was able to funnel funds toward its own proprietary system, which has meant that the inter-agency ITDS has been slow to get off the ground. Most recently, the Customs Service has gained jurisdiction over ITDS, taking it away from a joint-agency working group housed in Treasury. It is not clear that the system will now be implemented, or if it is, implemented as originally intended.

If implemented properly, these multi-agency systems could provide both information and services in a more streamlined and cohesive manner and make government run more effectively and cheaply. Yet, without new institutional means and leadership to support and promote these efforts, they are likely to be stillborn.

12 Principles for Implementing Digital Government

The Progressive Policy Institute offers the following 12 principles for implementing digital government.

1) Think Customer, Not Government Agency

Digital government both enables and requires rethinking how government is organized from the perspective of the citizen and the functions government performs to serve the needs of its citizens. A system based on functionality rather than agency jurisdiction, will lead to a more intuitive and efficient process of government-customer interaction where information is collected once and government functions are integrated. To do this, government must focus on customer requirements first and then work backwards to design systems that best meet those needs. The strategy should support the streamlining and integration of processes across the boundaries between government departments and agencies, so that those boundaries are invisible to the customer. This also means streamlining the processes between levels of government—federal, state, and local—so that cross-government applications are developed. Doing this will begin to reinvent the government's relationship with the public and will recognize citizens as real stakeholders. It will also raise citizen expectations of their government. Some nations have begun to use IT to reorient their gov-

ernment this way. For example, Australia called its report on digital government: *Clients First: The Challenge For Government Information Technology*.

2) Reinvent Government, Don't Simply Automate It

If digital government is viewed simply as a technology solution and is used to merely automate routine tasks, it will have failed to live up to its potential. Digital government must be part and parcel of government reinvention. The technologies need to be used to simplify government processes, drive internal change, and reorganize government.

For example, the Environmental Protection Agency is experimenting with allowing companies to file compliance forms online. But if the technology only makes the shift from scores of paper forms to scores of electronic forms it will not have taken advantage of the opportunity to use IT to reengineer government and move toward multi-media regulation (such as focusing on air, water, and solid waste emissions collectively).

3) Set An Ambitious Goal

In order to transform the federal government to a digital government, it is necessary to set an ambitious goal to be met in the near future. For example, Australia seeks to deliver all appropriate services on the Internet by 2001. British Prime Minister Tony

BOX C: Principles for Implementing Digital Government

1. Think Customer, Not Government Agency
2. Reinvent Government, Don't Simply Automate It
3. Set an Ambitious Goal
4. Invest Now to Save Tomorrow
5. Focus on Digital Transactions Between Citizens and Government
6. Make Government Applications Interoperable with Commercial Ones
7. Pass on a Portion of Savings From Electronic Transactions Back to Citizens
8. Promote Access to Information on the Internet, Do Not Restrict It
9. Respect the Rights of Americans for Information Privacy
10. Online Access to Government Should Not Eclipse Traditional Means
11. Federal Efforts Should Complement, Not Duplicate Private Sector Efforts
12. Take Action Now, and Learn From Mistakes

Blair declared in October 1997 that "within five years, one quarter of dealings with government can be done by a member of the public electronically—through their television, telephone, or computer." The 1998 Government Paperwork Elimination Act requires each federal agency to make its forms available for electronic submission by 2003 (through use of a digital signature when necessary).

4) Invest Now to Save Tomorrow

Investment in digital government will yield high returns as more time- and cost-efficient systems

are developed. However, Congress and the OMB too often view digital government appropriations simply as one expenditure competing against others. Moreover, appropriators usually expect immediate staff reductions from digital government, which are not possible until new systems are online and debugged, and the user community has switched. Expenditures on digital government need to be viewed as investments with positive returns in the near term.

5) Focus on Digital Transactions Between Citizens and Government

Internet enabled services should be the driver of digital government reengineering for the next five years. The growing popularity and availability of the Internet provides an unparalleled opportunity for the government to vastly improve contact with the American public. Government should ensure that all possible government-citizen and government-business interactions that can be transacted online are available.

6) Make Government Applications Interoperable with Commercial Ones

The driving force of information technology is interoperability—the basic foundation of the Internet. In embracing digital government, the government needs to make its systems interoperable with commercial ones rather than force the public to develop two separate systems—one for government use and one for private use. Interoperability makes the process of interaction more efficient, easier, less confusing, and cheaper for all parties involved. It also helps to resolve the chicken and egg problems slowing deployment of these technologies in the commercial marketplace.

7) Pass on a Portion of Savings From Electronic Transactions Back to Citizens

Digital government will save government money and these savings should be reflected in the "price" people pay for interacting with government. For example, Massachusetts offers a five dollar rebate on their driver's licence fee for those who register online, since it saves the state much

more. Providing rebates and discounts will encourage citizens to choose these lower cost forms of interaction. A United Kingdom survey found that a large proportion of the population is willing to use information technologies in interacting with government irrespective of their current knowledge or familiarity, provided that it offers benefits—including cost savings—to them.

Yet, the U.S. Government has not done this. For example, the U.S. Postal Service (USPS) will not give discounts to users of “electronic stamps” or postal meters, even though they cost the Postal Service less than purchasing stamps at a post office.⁷ Similarly, the IRS will not give a rebate for electronic tax filing.

Some argue that providing discounts will only benefit the affluent since they are now more likely to be on the Internet. Yet by lowering the actual cost of Internet access, rebates and discounts for online transactions (both government and commercial) will probably do more to get low-income Americans online than any other factor.

8) Promote Access to Information on the Internet, Do Not Restrict It

Moving to digital government will lead to issues regarding security and privacy. But if handled properly, these issues should be no more problematic than those faced in the current era of paper government. Yet, in the face of privacy concerns, elected and Administration officials can overreact, stymying progress. For example, a bill was introduced in the last Congress (HR1330) to prohibit government from providing information over the Internet. Rather than restricting online access to information, government should promote it and ensure that adequate security and privacy measures are in place.

9) Respect the Rights of Americans for Information Privacy

Some government entities have treated personal citizen information as belonging to the state, and have engaged in the practice of selling such information to the highest bidder, without citizen permission or knowledge. Examples have included prominent cases involving state driver's license lists and databases which have been sold

to third parties. The Supreme Court has ruled that such activity is unlawful, rejecting the defense by government that it ought to have the latitude to continue such practices.

As we make the transition to digital government, policies need to be put in place which ensure the privacy of the personal information of individual citizens. These issues are being addressed in the private sector through self-governance initiatives, including detailed “best practices” certifications by groups as Trust-E and BBB-OnLine. Governments should do no less to ensure that their own practices respect the privacy of citizens. In addition, as the federal government becomes more digital, it needs to ensure that it has top-quality security systems in place which protect the integrity of information against hackers and other threats. Specific policies of this sort, and funding to support them, are necessary to help instill public confidence in governments' intentions in the evolving Information Age.

10) Online Access to Government Should Not Eclipse Traditional Means

All services that can be provided digitally should be. However, at least for the foreseeable future, federal services should remain accessible through all forms of communication, including mail, phone, and in person, for those who cannot or do not wish to communicate digitally. For example, an individual should still be able to call the Social Security Administration office to find out how to apply for benefits, even when the information and application process is online.

11) Federal Efforts Should Complement, Not Duplicate Private Sector Efforts

In OMB Circular A-76, nine successive American presidents, beginning with Dwight Eisenhower, have set forth a policy regarding the relationship of government to the performance of “commercial activities.” That policy is well-summarized in one sentence: “A commercial activity is not a governmental function.”

As the federal government ventures into digital government it needs to remember the A-76 guidelines. In some instances, government agencies have recently pursued strategies where good

electronic government ideas have evolved into electronic commerce initiatives, where the government took on a role of providing commercial products or services to consumers in competition with the private sector. Whether the subject is the USPS and electronic bill presentment and payment, or a state agency with electronic tax preparation services, or a federal department wanting to commercially sell its electronic payroll services, these forays cross the line into electronic commerce.

For example, it is one thing for government to provide tax forms in electronic format (as they already do in paper format), it is quite another to provide tax preparation software that mimics the functions of tax preparers. Similarly, it is one thing for the USPS to use information technologies to support its mission of delivering physical mail. It is quite another to become an Internet Service Provider. For example, the USPS has announced an interest in entering the market for electronic bill presentment and payment services. Yet, it is not appropriate for the USPS to unilaterally expand its charter beyond the delivery of physical mail and packages and to compete with private sector companies already providing such services as e-mail, electronic carrier services, electronic certificate authorization, or electronic bill presentment and payment.

The justification government agencies often make for such efforts is that they are simply acting more like private corporations, and after all, isn't this the goal of government reinvention? Yet, when reinventing government advocates argue that government should operate more like a business, they mean that it should become effi-

cient, faster, and more customer-oriented in its delivery of services—not that it should effectively go into business and use public funds to competitively provide commercial goods and services in private markets.

As a result, digital government efforts should be focused on those innovations and initiatives which are necessary to fundamentally improve service to the citizen in inherently governmental functions, and to provide significantly better access to public information resources. Public funds, whether appropriated by Congress or generated through systems such as the Postal Rate Base, should not be used as venture capital to launch governmental agencies into competition with the private sector. There are too many necessary functions of government which are either going unfulfilled, or are being poorly performed in outmoded ways, to be able to justify in an era of limited budgets spending taxpayer dollars on activities which fundamentally change the role of government in our economy.

12) Take Action Now, and Learn From Mistakes

The IT revolution is changing so rapidly that waiting until the “perfect” comprehensive system can be developed will mean that any solution will be out of date by the time it is implemented. Government needs to move forward with smaller projects that, if successful, can be scaled up. Moreover, failure should be seen as an opportunity to learn what does not work, and not necessarily something to be penalized.

Policy Recommendations

To accelerate the pace of transformation we recommend that the Congress and the Administration do four major things to foster digital government:

1. Establish the Position of a Chief Information Officer for the Federal Government
2. Establish a \$500 Million Annual Digital Federal Government Fund to Invest in Cross-Agency Digital Government Projects
3. Give Agencies the Flexibility in the Use of Funds for Digital Government and Let Them Keep the Savings Generated by It
4. Expand Funding for Agencies to Develop Digital Government Applications

Establish the Position of a Chief Information Officer for the Federal Government

Currently, 54 federal agencies have CIOs, but the federal government as a whole does not. Current coordination efforts are just that, meetings among equals without the budget or authority to implement government-wide digital government solutions. A federal CIO would report directly to the President and direct the process of developing a concerted digital government conversion plan. He

or she would have a budget independent of individual agencies to help drive the next generation of digital government, much of it involving cross-agency applications. The CIO would head inter-agency and cross functional IT councils. The office would also take the lead in shaping the Administration's policy regarding the Internet, oversee issues of computer and network security for the government, and work with state and local governments to promote digital government. Just as the Y2K "tsar" was able to assert strong leadership in dealing with a potential Y2K crisis in government, a federal CIO and a comprehensive plan will foster digital government in a faster, more effective, and more comprehensive manner.

A number of states and nations have moved in this direction, appointing technology directors. For example, British Prime Minister Tony Blair has appointed an e-minister to coordinate the various departments involved in developing digital government as well as carry out e-commerce initiatives to improve service to the citizens.

Establish a \$500 Million Annual Digital Federal Government Fund to Invest in Cross-Agency Digital Government Projects

Agencies generally have not funded interagency digital government projects. Similarly, appropriations by both Congress and OMB is organized by

Box D: Ten Digital Government Applications

There are literally hundreds, if not thousands, of applications that could be developed to allow businesses, citizens, and other governments to interact with the federal government digitally. Here are 10 examples of things that could be done today.

1. Businesses and individuals could file tax returns directly with the IRS at no cost.
2. Exporters could fill out just one electronic form that is automatically routed to all government agencies involved in export issues.
3. Individuals could bid on government surplus items online.
4. Companies could file environmental compliance forms online.
5. Individuals could apply for Social Security benefits online.
6. Businesses could query a computerized "expert system" to find out what regulatory requirements their particular facility faces.
7. Individuals could store and access their medical information on a "smart card."
8. Individuals could search for federal employees through a centralized and integrated online database.
9. Government officials could purchase goods using electronic catalogs.
10. Companies could access and bid for government procurements on the Internet.

department, not function, so finding allocations for cross-agency projects is difficult. Only a small amount of funds for agency pilot projects has been allocated. But while pilot projects can get programs launched, they are not able to sustain them or develop them on the scale needed.⁸ Providing a pool of funds specifically targeted at implementing significant cross-agency projects would not only provide the resources to implement such projects, it would provide the organizational direction to get them done. However, to ensure agency buy-in, agencies should be required match these funds. And Congress should allocate funds to agencies specifically targeted to joint projects.

Give Agencies Flexibility in the Use of Funds for Digital Government and Let Them Keep the Savings Generated by It

Digital government will save money, but where will the government get the money to implement this

innovation? There is a model from the private sector. A number of computer/IT service firms, led by IBM and EDS, contract for these services with companies and, in effect, guarantee productivity gains to the firm. In return, companies are compensated out of a portion of the client firm's productivity gain.

Current law allows federal agencies to contract for energy efficiency technologies that will lower energy costs, with the contractor being paid out of the agency's energy cost savings. In this way, the agency doesn't have to invest up-front appropriated monies in efficiency saving technologies. Rather, it can pay for them over time with a part of the cost savings. The Clinger-Cohen Act of 1996 similarly allow federal agency pilot experiments with such "shared savings" contracting in the information technology area.

The information technology provision hasn't been used yet, probably because there is no "up side" for the agency—it has to return any savings to the Treasury, and can't use savings to enhance

its mission responsibility. But if that provision were fixed, and if broader demonstrations were permitted (rather than just the two pilots the law currently allows), this might be a significant way to expand digital government.⁹ In particular, agencies should be allowed to earmark the savings from digital government to their own innovation funds to finance further digital government initiatives.

In addition, governmental agencies should be given increased flexibility regarding digital government-related procurement. The Administration should identify pilot digital government projects that meet certain requirements, and develop new acquisition and procurement methods for them that are faster and more flexible. For example, in 1999 Congress gave the Central Intelligence Agency the authority and funding to create a \$28 million "venture capital fund" to help generate and procure advanced information technologies to help the agency carry out its mission.

Expand Funding for Agencies to Develop Digital Government Applications

Federal funding for information technology has grown every year since 1996, but the rate of growth has slowed, while the amount going to new applications has declined. In FY96, federal funding for information technology grew almost 8 percent, while in FY2000, it grew less than 2 percent, increasing slightly more than 4 percent in the President's 2001 budget.¹⁰ Moreover, this growth has not kept pace with growth in private sector information technology expenditures which have averaged over 8 percent growth per year through 1999.¹¹ In addition, much of the increase in funding for IT has gone to maintaining existing systems (increasing 24 percent between FY99 and FY01), while funding for modernizing and developing new systems has actually decreased 2 percent.¹²

What Government Is Doing Now, What Government Should Be Doing

There are at least three distinct aspects of digital government: information dissemination, interactive service delivery, online monetary transactions. This section details what the government is doing in each of these areas and suggests what government policy makers and managers should be doing.

Information Dissemination

What the Government is Doing

Government has begun to embrace the Internet, but most applications still focus on information dissemination from the government to the user. The information dissemination capabilities of the Internet and the low cost of maintaining and updating web sites has helped substitute for a shrinking government budget. Every federal agency from the statistics-rich Department of Commerce to the secretive National Reconnaissance Office maintains news updates, background information, and other data accessible through the Internet.

However, the lack of coordinated IT policy has created disparities and duplication in the trans-

fer of online information between agencies. While some agencies stand out as innovative service providers, most do not utilize the Internet to its full capability—often viewing the Internet as a tool simply for *information dissemination*, and not a means of carrying out complex transactions. Moreover, agencies vary significantly in how online information is organized and the web site designed, making finding information confusing. While most agency web sites maintain individual search engines, they are of varying capability and efficiency, some allowing advanced searches while others have few customizing capabilities.

Most government web sites are designed with an agency-centric focus, not a customer-centric focus. For example, the typical agency web site home page features a picture of the department secretary, and lists press releases and other recent news about the department. This is equivalent to the Amazon.com home page featuring a picture of its CEO Jeff Bezos, along with press releases on how well Amazon's stock is doing, instead of immediately seeing how to buy books, CDs, etc.

Information is often quite difficult to find unless one is lucky enough to know what agency or bureau to look at.¹³ In response, the federal gov-

ernment has developed some "portal" sites that aggregate a variety of information. Sites such as *business.gov* do a reasonable job of organizing government-related information that businesses may need. However, while they provide numerous resources from obscure technical information to general knowledge information, most federal portals (e.g., *webgov.net*; *fedworld.gov*) are confusing, difficult to use, and do not comprehensively and accurately search all online government documents. More importantly, most are simply collections of many disparate web sites, as opposed to means to truly organize federal information in logical and accessible ways. In this sense, these sites are currently pointers to agency-centric organizations and their services, not real vertical and horizontal portals organized according to how customers view and seek government services and capabilities.

Moreover, because individual agencies and programs develop their own web sites, there is duplication of efforts. For example, both Access America's student web site (*students.gov*) and the Department of Education's Easy Access for Students and Institutions (EASI) web site¹⁴ focus on students, but the EASI web site does not link to the Access America site and its online student loan application function. The proliferation of agency and program-specific web sites is a reflection of the stovepipe nature of the federal government and the inability to organize information and services around the customer. As the federal CIO Council states, IT has been "used in pockets of isolation to accomplish separate and distinct tasks."¹⁵

Several agencies are beginning to combine resources to better carry out tasks, record transactions, and benefit the consumer. As stated earlier, Vice President Gore's National Partnership for Reinventing Government (NPR) has been at the center of the efforts to reform government and traditional agency practices. Specifically, NPR's Access America program has worked to coordinate government-wide resources into a more user-friendly structure, namely in the form of gateways (web sites pertaining to a particular topic) focused on seniors and students. The resources are primarily links to online information such as Social Security benefits, educational resources regarding scholarships, and federal loans. But there are few

innovative services available on either gateway and a number of links seem to be quite dated.

What Government Should be Doing

- **Develop an enterprise-wide information architecture:** In an attempt to make web sites more easily accessible, the Australian and Israeli governments have developed design and content standards for their web sites.¹⁶ Simple baseline standards on design, file architecture, and information display for federal web sites will make it easier for users to navigate sites and retrieve information. This should be part of a broader effort to develop a shared information architecture for the federal government that addresses issues of data sharing, telecommunications usage, and standards for web design.
 - **Implement a standardized information tagging system.** Most indexed information cataloged by an Internet search engine is retrieved using search programs (called spiders or robots) which explore the World Wide Web by tunneling through web pages and categorizing the information contained therein. The degree and depth to which the robots search differs from engine to engine. The process is time consuming (considering the billion-plus web pages) and results in an index of web sites which are often not accurately organized according to relevance. Increasingly, web developers have begun adding metatags, or short descriptions of the web page content, for use by search engines in cataloging web pages. However, there is currently no standard for Internet metatagging.
- The most effective solution for categorizing information on government web pages would be to develop a database-driven system, where all information is automatically listed in databases as it is placed online. Implementing this type of system would allow more accurate and efficient searches. Extensible Markup Language (XML), a newly approved Internet standard for developing highly interactive and flexible web pages, will allow a more accurate and efficient categorization for improved indexing and searching.

However, while XML is a viable solution to information organization, it will take time to implement and does not solve the current problems associated with indexing. In the interim, a metatagging standard should be developed that will more accurately index immediately forthcoming and currently available web pages. The standard should be applied to all government web sites to improve government-wide search agents, and should be available to commercial search engines to better enhance their search capabilities.¹⁷

The federal government should consult with several organizations currently working on metatagging initiatives and either support one standard or develop one for government use. Combining metatagging with the capabilities of XML will allow expert systems, intelligent agents, and next generation search engines to use semantics and concept association to search and index information.¹⁸ For example, this type of technology could be used by the Department of Health and Human Services and others to establish health information networks; where people could get state of the art health information online despite not knowing complex medical terminology and jargon (see Box E, p.18).

- **Create an entryway/portal to government services.** Web sites need to be categorized by the function of the service rather than the agency (or most likely, agencies) administering them. A well designed portal to all online federal information will make citizen-government interaction more efficient and effective. But a portal needs to be more than simply a mega-link to government web sites. Rather, it needs to completely bypass agency stovepipe organization and be organized by information and type of interaction.

Australia¹⁹ has organized a central web site by bringing together eight different government programs into one web site interface for the citizen, called CentreLink. The Israeli government completed a similar process and created a portal to Israeli government services.

- **Expand the amount of information acces-**

sible on searchable databases. The federal government has an enormous amount of information in databases, but most are not searchable online. For example, citizens should be able to search Bureau of Land Management land records to identify land parcels. In fact, there are a host of potential database functions that could be developed.

- **Use "information on request" to provide people with government information.** This notification technology automatically sends information to individuals based on criteria that they have submitted which is unique to their interests. For example, companies should be able to answer a questionnaire and automatically receive an e-mail informing them of each federal procurement solicitation that matches the criteria they entered. Similarly, this technology could inform businesses of new regulations that might affect their particular facility or company.
- **Develop "expert systems" to access information.** Expert systems are software programs that let individuals enter information and receive back expert advice based on the data programed into the software. For example, the Occupational Safety and Health Administration has developed a series of online "adviser" expert systems to help business people to identify safety problems in the work place—from cadmium to mercury to asbestos—and determine an appropriate course of action.²⁰
- **Make the Web the first place to put information, not the last.** Too many federal web sites are "stale," only slowing adding new information and in many cases containing information that is months and often years out of date. For example, one agency site describes its efforts to use Electronic Data Interchange (EDI) protocols to allow companies to file regulatory information, even though the information is years old and the agency is now planning on using Internet-based systems. Agencies need to post information on the web even before they publish it in other forms.

BOX E: Creating Health Information Networks²¹

As purchaser of about half of the nation's health care (through Medicare, Medicaid, the VA etc.), the government is in a unique position to catalyze greater adoption of information technology throughout the health care system. Indeed, in the Information Age, affecting the change outside your organization is as important as the change inside it. And nowhere is this more apparent than the health care system.

Consider how many times patients must fill out medical histories. Each doctor and hospital has their own form and no system for checking the accuracy of the records. Yet such information can literally be a life and death matter for patients. As one business leader put it, an ATM knows more about your finances than the average doctor knows about your medical history.

The Department of Veterans' Affairs has taken the lead in catalyzing adoption of information technology for health records. The leaders of the VA have come to realize that any information system that works only in their own system won't do them any good. Even VA patients do not stay in the VA system, so if doctors are to track their patients, they need a system that everyone can use.

The VA's goal is much like the DOD's in building the Internet. The DOD needed a communication system that couldn't be shut down by the enemy because it was widely used yet controlled by no one. The VA realizes that any system for exchanging health information must be similarly diffuse in order to operate between the highly fragmented elements of health care, and cannot be controlled by any one element of the health care system, which few people would trust.

As VA health care consultant Tom Munnecke puts it, everyone should be able to have a personal health space that allows for the secure, private, and confidential exchange of health information from their medical history to the payment for health services. It might take the form of a personal web site where consumers could keep and control access to their health records, communicate confidentially with their doctor or other patients with similar health problems, and shop for health care services that are best matched to their needs and preferences.

The key to creating a personal health space is an organization that reflects the diversity of the health care system and yet comes together around a common purpose of giving people control of their health and health care. Along with the VA, other federal agencies and private sector organizations like the American Hospital Association have launched the "Vvaleo" project. Vvaleo is from a Latin word, "to be in good health." While it is still in the very early stages, this organization or another like it is needed to address the systemic problems in health care that otherwise slip through the cracks because no one is directly responsible for them.

The government must also assure that personal health information is not abused. Incredibly, there are no national laws or even national standards on health information privacy and confidential use. While a national regulatory process is underway as part of the Health Insurance Portability and Protection Act, it covers only electronically stored information and not written records, which could potentially create an unlevel playing field and effectively discourage using information technology to replace written records.

- Measure customer satisfaction.** Just as its possible to get data on the number of times private web sites have been visited, it would help assess the usefulness of federal web sites by tracking and reporting this information. Usage metrics should be built into the site maintenance process. In addition, all web sites should have standardized ranking forms built into them where citizens can rank a web site (1 to 5, with 1 being extremely useful, and 5 being not useful) on how useful it is to them and to what degree it met their needs. These will help government customize its efforts to meet citizen needs.

Interactive Service Delivery

It is one thing to simply provide information on a web site, it is another to allow businesses or citizens to engage in transactions with the government. Creating an agency web site is relatively easy. But government must do more than this, it must enable citizens to interact and transact business with government. But this is harder, both technically and organizationally. It is not good enough to simply build a fancy web site with online forms for people to fill out and submit if the forms are printed out (on the government end) and go into the same old bureaucratic system. The government must reinvent itself the same way companies have had to reinvent themselves in the private sector: use the technology to replace bureaucracy with more efficient systems and more flexible human organizational structures. Online transactions are the next major challenge to implementing digital government.

What the Government is Doing

The online form has become one of the preeminent Internet-age tools for web-based communication; a fundamental step toward improving online services. Using an online form, a person can submit information which is deposited directly into a database, saving both the person and the organization time and money. The range of applications and the cost savings and quality improvement (reduced errors) are immense.

Many agencies allow individuals to obtain forms online, print them, and then mail the paper copies, where the information is then either entered by hand or scanned into a computer.²² A few agencies are beginning to allow citizens and businesses to file forms online. For example, the Postal Service allows residents to file change-of-address forms online, while 18 year-old American males can register with the Selective Service online to immediately obtain a Selective Service number. The Social Security Administration also maintains an online benefits calculation service (however, the information is mailed to the applicant). The National Park Service allows people to make registrations online. In addition, some federal agencies, such as the Securities and Ex-

change Commission, the Federal Communications Commission, and the Federal Energy Regulatory Commission allow companies to submit regulatory filings online.

What Government Should be Doing

- **Expand and standardize the number of applications for online forms.** All government forms should be publicly available and searchable on a central federal web site. The 1998 Government Paperwork Elimination Act requires each federal agency by 2003 to make its forms available for electronic submission (through the use of a digital signature when necessary). President Clinton recently issued an executive memorandum to all executive departments and agencies calling for the availability of online forms needed for the top 500 government services by December 2000.²³ There are a host of potential applications including: applying for Social Security benefits, veterans benefits, passports, and federal jobs; allowing businesses to pay Social Security and other regularly recurring taxes; allowing people to respond to government surveys (e.g. Census); and letting attorneys file federal court documents electronically.
- **Whenever possible, use Web-based technology.** In the private sector, e-commerce applications are evolving toward the web, and away from proprietary electronic data interchange (EDI) protocols managed by fee-based vendors. Yet some federal applications have been slow to move toward web-based applications, even though they do not require costly subscriptions to EDI Value Added Networks and are more accessible to small businesses and individuals. Forms packages should also have open standards so that they all tie into back-end legacy systems.
- **Online forms should use shared information about the submitter.** One of the frustrations many individuals experience with e-commerce is the requirement to fill in personal information every time they order something online. E-commerce vendors are working on solutions that would allow indi-

viduals to only enter personal information once, saving them time and effort. Directory technology such as Lightweight Directory Access Protocol (LDAP) is used to maintain one information resource that is queried by multiple systems. This system should be used in conjunction with XML or other advanced and flexible Internet-related formats. The federal government needs to adopt the same system so individuals can streamline their interactions with government.

- **Integrate forms.** Putting forms online is one thing, streamlining and consolidating information collection is another. For example, EPA has been slow to shift to one-stop reporting whereby companies fill out one form, ideally for both state or federal compliance reporting. The proposed International Trade Data System is an example of this (see Box B, p.6).
- **Focus on intergovernmental solutions.** Many online applications require citizens and businesses to deal with multiple levels of government. For example, companies must file local, state, and federal environmental regulatory compliance forms. Digital government efforts need to be integrated at all levels of government to streamline these processes.

Online Monetary Transactions

Monetary transactions increasingly rely on electronic funds transactions (EFT). This process significantly reduces transaction costs and improves the timeliness of interaction. The federal government is the largest issuer of checks and is the largest procurer of goods and services in the world. Virtually all of these activities could be done electronically, replacing paper.

What the Government is Doing

Government has begun to embrace online monetary transactions. For example, the IRS encourages online filing of tax returns for both citizens and businesses. Online filing reduces instances of data error from an average of 21 percent (in paper) to less than 1 percent, and significantly reduces the transaction costs of processing returns and checks.²⁴ In 1998, 24.6 million Americans—

an increase of 28 percent from the year before—filed their tax returns electronically.²⁵ However, due to a lack of digital signature protocol, the user is required, via mail, to return a signed confirmation sheet to the IRS. The IRS also uses direct deposit of refunds, saving substantial costs. The costs of issuing a paper check are \$2-\$3.50 per check, compared to roughly \$0.15-\$0.55 with direct deposit and EFT.²⁶ Despite the convenience and cost savings of e-filing, it was not until January 2000 that the first business tax return was submitted online; and even then, only one company has been authorized to process electronic tax returns for businesses.²⁷

Today, a large share of federal payments (except tax returns) are carried out through EFT, as required by the 1996 Debt Collection Improvement Act.²⁸ In FY99, 68 percent of government payments, including benefit payments, were transacted through EFT; additionally, 96 percent of salary and allotment payments were carried out using EFT.²⁹ Savings after full conversion to EFT could reach roughly \$100 million per year.³⁰

The government is also embracing electronic benefits transfer (EBT) to convey medical, food, and other government-to-citizen benefits. Increasingly, electronic benefits are placed on debit cards or smart cards. Like EFT, EBT replaces the need for checks and allows people receiving government support to have it automatically transferred to debit cards. This is especially useful for the 20 percent of benefit recipients who do not have bank accounts. Today, 39 states—29 of which are state-wide programs—use EBT systems with benefits going to 4.25 million families (\$1.35 billion per month in food stamp benefits alone).³¹ The National Partnership for Reinventing Government has proposed putting all (federal and state) benefit-related information on one card, to reduce confusion and cost, and increase convenience.³² One of the most innovative pilot programs, which incorporates state, local, and federal government benefits, has been the Health Passport, a project developed by the Western Governors' Association. This program places all medical benefit information on one smart card and can be used to redeem a variety of benefits—from medical care, to pharmaceutical products, to food benefits.³³

As the world's largest purchaser, the U.S. Government spends large sums on procurement.

E-commerce cuts the costs of procurement and acquisition for government and for vendors. The majority of government agencies have unique procurement and electronic catalog systems, utilizing non-web based proprietary accounting and data basing software. Department of Defense is perhaps farthest along, having established a goal of an entirely paperless contracting system for major weapons systems by January 2000.³⁴ The Federal Electronic Commerce Program Office and the Interagency Acquisition Internet Council are working with CommerceNet,³⁵ an electronic commerce industry membership organization, to develop interoperable electronic catalogs which allow agencies to post notifications of their needs online for public bidding by contractors. The catalogs would also allow companies to list goods and prices for government purchasers. Currently, vendors can go to the electronic posting system (*eps.gov*) where agencies post their procurement requirements for purchases above \$25,000. The General Services Administration (GSA) hopes to have this system in place on a government-wide basis by early 2001. Similarly, *fedcommons.gov* is a gateway to a large share of government grants that are awarded.

The government is also beginning to experiment with allowing individuals to purchase items from the federal government online. For example, in its first month online, the U.S. Mint averaged sales of \$2 million per day of numismatic sets and coins. Savings bonds can be purchased online. Individuals can also buy stamps, postal products, and savings bonds online.

The government is also beginning to use smart cards to fulfill an increasing number of functions including EBT and procurement. Integrated circuit chip cards, or smart cards, enable the centralization of information, tools, and identification on one small plastic card. The cards are being used by the private sector, and increasingly by the government in pilot programs, as a means of organizing several card-based tools onto a single card.

The Department of Defense (DOD), especially the Navy, has begun to implement smart card technology for American servicemen. Smart cards make obsolete the multiple forms and papers servicemen are required to keep. The Navy uses smart cards for identification, ATM-at-sea cash re-

trieval systems, medical and dental records, retrieval of classified documents, and accountability tracing of government tools and clothes by Navy personnel. Proposed improvements will include tracking mess line attendance, debit card capability with the ship's store, and recording mail room pick-ups.³⁶

The private sector has been anxious to work with government on the development of smart cards. Citibank, IBM, Visa, 3G International, GTE, the Sandia National Labs, and the Federal Technology Service have created a 500-card pilot project for Federal Technology Service employees in Virginia. The 16KB card includes the basic utilities of smart cards: ID, building access, procurement ability, calling card, access to LAN and applications, as well as direct access to airplane boarding.³⁷

What Government Should be Doing

- **Use EFT in all monetary transactions.** Electronic fund transfer will save government, citizens, and businesses both time and money. This process also automatically creates an accurate record of transactions.
- **Implement the use of electronic checks.** Electronic checks involve not just the transfer of funds but also the transfer of an electronic record to the recipient. The Treasury Department is in the initial stages of a trial program using this technology; this should be expanded government-wide.³⁸
- **Develop government-wide electronic procurement systems.** A standardized electronic procurement system would reduce costs and increase competition and convenience. The process would include bidding by companies for government contracts, as well as search engines and virtual assistants which will help government employees find desired goods at the lowest possible prices. The "Channel Convergence in a Delivery to the Citizen Model Pilot" with the Social Security Administration is focusing on this area.
- **Issue government benefits through EBT.** Automatic allocation of benefits will reduce pa-

perwork, cut costs, and allow government to keep better track of benefit use for data and studies. States that have not yet implemented EBT programs should work with both the federal government and the private sector to develop systems.

- **Expand the number of items citizens can purchase online.** To the extent that federal agencies sell items, citizens should be able to purchase them online. CommerceNet is working with the federal government to allow citizens to find online government surplus items. In addition, the government should develop an online auction for disposing of surplus government property. Other applications should be developed.
- **Make it easier for citizens and businesses to directly file their taxes online.** Simply continuing the current system of regulating the certification of data transmitters who batch income tax returns and submit them by proprietary tax agency electronic protocols is not adequate. Governments should instead invest in the 'back room' infrastructure necessary to permit direct electronic transmission to the government of completed tax returns by individual citizens using their private sector software. The creation of such electronic portals will also facilitate direct electronic communication between citizens and tax agencies, allowing citizens to access general government information, information on tax return status, and individual income tax "accounts." Digital government in the income tax environment cannot move forward in robust ways until the government invests in modernizing the infrastructure underlying the entire tax system.
- **Expand federal smart card applications.** Currently, smart cards are in use in pilot programs. Pending successful outcomes, these card applications should be expanded. For example, the Veterans Administration could issue smart cards to veterans to obtain prescriptions. In addition, the smart card can also house the veteran's medical history and other information. In fact, there is no reason why this could not be extended to all Americans who could have their medical history on one card. The government should explore how to extend benefits and services to all Americans through the use of smart cards.
- **Ensure that government smart cards are interoperable with private sector applications.** At minimum, government smart cards need to be interoperable with other cards in government. Ensuring that government smart cards can be used in non-governmental applications will help jump start the introduction of smart card technology and smart card readers throughout society, making it a more useful tool for government use.
- **Attach digital signature functions.** Attaching digital signature (i.e. online authentication) abilities to smart cards (along with a password) would allow verification for forms and transactions and would help jump start the use of digital signatures.³⁹

Conclusion

The U.S. economy is going digital. This information technology revolution provides the opportunity for the federal government to transform itself and the way it provides services to citizens. Doing so would not only cut the cost and improve the quality of government, it would improve the trust citizens have in their government. Yet, real progress in a timely manner depends upon digital government rapidly becoming a priority of Congress and the Administration, both in terms of funding and leadership.

Endnotes

- ¹ The IRS reports that it costs \$3.50 to mail out a tax form, compared to 2 cents on the web. Hewlett Packard reports that it would save \$1 million per year for filing just one form electronically: the W-4 (dependent declaration tax form for taxes). Press Release from the Office of Congresswoman Anna Eshoo, "Congress Passes Eshoo's Landmark Digital Signature Legislation" October, 28, 1999 (<http://www.house.gov/eshoo/digsigw.htm>).
- ² As of January 2000, 45 percent of American households were online. Strategis Group, *U.S. Households with Internet Access to Nearly Doubly to 90 Million by 2004*, (February 8, 2000) and U.S. Census Bureau, *Projections of Households by Type: 1995-2010* <http://www.census.gov/population/projections/nation/hh-fam/table1n.txt> (May 1996).
- ³ This box was written by Debra Knopman, director of the Progressive Policy Institute's Center for Innovation and the Environment.
- ⁴ Thomas W. Lippman, "U.S. Diplomacy Behind the Times, Studies Say," *Washington Post*, (10-28-98).
- ⁵ There are numerous smaller committees and organizations such as the Federal Communicators Network and the Federal Webmasters Forum which tackle more focused IT issues.
- ⁶ President William Jefferson Clinton, "Memorandum for Heads of Departments and Agencies: Electronic Commerce" (December 17, 1999).
- ⁷ Similarly, while the Postal Service gives discounts to businesses who bar code mail, they do not give them to consumers who mail bar coded envelopes (e.g., return envelopes of bills).
- ⁸ Currently, the GITS board oversees a small Information Technology Innovation Fund to fund cross agency projects, but at less than \$7 million per year, the funding does not go very far. The funds come from a small agency "tax" on their FTS2000 long distance telecommunications budgets.
- ⁹ William B. Bonvillian, Speech given to the National Academy of Sciences/National Research Council Symposium on Government-Industry Partnerships in Biotechnology and Computing (October 25, 1999).
- ¹⁰ Tom Hewitt, Federal Sources, Inc. *Virtual Government 2000*, Presentation to the AFCEA Virtual Government 2000 Conference, Washington, DC: February 23, 2000.
- ¹¹ Ibid.
- ¹² Ibid.
- ¹³ For example, the National Science Foundation maintains scores of studies and reports on scientific issues as well as on aspects of the science and technology sectors. From education to employment, the CIA maintains a huge database of country-specific information. *Fedworld.gov*, an online federal information resource (maintained by the Department of Commerce) lists over 20 databases maintained by various federal agencies.
- ¹⁴ <http://easi.ed.gov/>.
- ¹⁵ Chief Information Officers Council, *Strategic Plan, Fiscal Year 2000*, p. 2.
- ¹⁶ Australia: <http://www.fed.gov.au/>. Israel: <http://www.info.gov.il/eng/mainpage.htm/>.
- ¹⁷ Malcolm MacLachlan, "Meta-Tagging May Improve Web Searches," *TechWeb* (April 17, 1998) (<http://www.techweb.com/news/story/TWB19980417S0018>).
- ¹⁸ Laurie Ann Toupin, "Software That Does Your Research For You," *Design News* (September 20, 1999) (<http://www.manufacturing.net/magazine/dn/archives/1999/dn0920.99/18f1907.htm>).
- ¹⁹ <http://www.centrelink.gov.au/>.
- ²⁰ <http://www.osha-slc.gov/dts/osta/oshasoft/>.
- ²¹ This box was written by Dave Kendall, senior fellow for health policy, Progressive Policy Institute.
- ²² For example, the U.S. Copyright Office allows individuals to download registration forms and submit them by mail (<http://www.loc.gov/copyright/forms/>).
- ²³ The White House, "Memorandum for the Heads of Executive Departments and Agencies: Electronic Govern-

Digital Government

ment," (December 17, 1999).

²⁴ http://www.irs.gov/elec_svs/fed_state.html/.

²⁵ *A Strategy for Growth*, The Electronic Tax Administration (December 17, 1998) (http://www.irs.ustreas.gov/prod/elec_svs/eta-plan.html).

²⁶ Larry Carnes, *Electronic Delivery of Government Systems*, General Services Administration (June 1998) p. 23.

²⁷ "The Tax Man Takes it Online," *National Journal's Technology Daily*, (February 10, 2000).

²⁸ <http://ec.fed.gov/eft.htm/>.

²⁹ <http://www.fms.treas.gov/eft/agency/VFY99.html/>.

³⁰ <http://www.fms.treas.gov/eft/>.

³¹ <http://ec.fed.gov/ebfacts.html/>.

³² <http://ec.fed.gov/ebfacts.html/>.

³³ <http://www.westgov.org/wga/initiatives/hpp/>.

³⁴ <http://www.acq.osd.mil/pciplt/>.

³⁵ <http://www.commerce.net/>.

³⁶ <http://www.doncio.navy.mil/focusareas/smartcard/index.html/>.

³⁷ <http://smart.gov/section04e.htm/>.

³⁸ <http://www.echeck.org/>.

³⁹ Marc Strassman and Rob Atkinson, *Jump Starting the Digital Economy* (Washington, DC: Progressive Policy Institute, 1999) (<http://www.dlcppl.org/texts/tech/privacy.htm/>).

About the Authors

Dr. Robert D. Atkinson is director of the Progressive Policy Institute's project of Technology & New Economy. Previously he served as executive director of the Rhode Island Economic Policy Council, and as a project director and senior analyst at the Congressional Office of Technology Assessment (OTA). While at OTA, he directed the Technological Reshaping of Metropolitan America, a report examining the impact of the technology revolution on America's urban areas. Dr. Atkinson holds a Ph.D. in city and regional planning from the University of North Carolina at Chapel Hill.

Jacob Ulevich is the Project Assistant for the Progressive Policy Institute's Technology & New Economy Project. Prior to joining PPI, he worked at an export control consulting firm and designed web sites for the Washington College of Law. Mr. Ulevich is a recent graduate of American University.

Acknowledgements

The authors wish to thank the following individuals for reviewing and providing comments on earlier drafts: Kaye Caldwell, Ron Parsons, Leslie Lundquist, and Dave Hollander, Commerce.net; Isreal Feldman, President, Council for Electronic Government; Jane Fountain, Professor, Kennedy School of Government, Harvard University; Brian Kahin; Bruce Heiman, Preston Gates Ellis LLP; Chris Caine, Tim Sheehy and Kathleen Kingscott, IBM; Elliott Maxwell and Alan Balutis, U.S. Department of Commerce; Bernard McKay, Intuit Corporation; Marty Wagner, General Services Administration; David Osborne; Alan Procter, Lexus-Nexus; and Chuck Alston, Debbie Boylan, Randolph Court, and Will Marshall, PPI.

Mr. HORN. When I was a university president, I had a CIO in 1971, and I began to wonder what's the fuss, folks, we did that 20, 30 years ago on every single decision before the university. He sat right at the management group. And it's about time that we got some focus on that in the executive branch.

Now, our next presenter comes with great credentials that we all respect: William Scherlis, principal research scientist, School of Computer Science at Carnegie Mellon University. And Carnegie Mellon has done a marvelous job in working on just the issues that we're concerned about, so we're delighted to have you here.

STATEMENT OF WILLIAM L. SCHERLIS, PRINCIPAL RESEARCH SCIENTIST, SCHOOL OF COMPUTER SCIENCE, CARNEGIE MELLON UNIVERSITY

Mr. SCHERLIS. Thank you, Mr. Chairman.

Mr. Chairman, Mr. Turner, Mr. Davis, thank you for the opportunity to appear today on this issue of the definition and role of the Federal CIO. My focus in this testimony is on innovation in government information technology. I am emphasizing innovation because I believe that we will not be able to realize the vision of government online, unless there is a new kind of leadership. Nor will we successfully address our security challenges.

In particular I support the creation of a Federal CIO within the Executive Office of the President who can exercise positive leadership with respect to multiagency efforts, new kinds of customer-focused services, innovative acquisition processes and appropriate technological and architectural innovation.

I'm going to make quick comments on each of these areas, but first the bottom line, which is that the Federal CIO must be empowered to provide this positive leadership. The empowerment should come from direct access to funds, agency funds which are used by the Federal CIO to leverage in order to buy down risk for innovative projects, for multiagency projects, and for exploratory projects. The process would be led by the Federal CIO, but administered and managed in individual agencies by agency CIOs. This would enable the Office of the Federal CIO to be a lightweight operation within the EOP along the lines envisioned in both of the proposed bills, H.R. 4670 and H.R. 5024.

Why do we need this positive leadership? We need it in order to respond to several challenges. The first is customer-targeted services and multiagency efforts. Starting and managing a small business, for example, requires an entrepreneur to interact with multiple agencies—in the present regime—and to develop a deep knowledge of the roles and structure of those agencies involved. It would be much more effective to offer one-stop shopping, and this is now being done in many States. The State of Washington, for example, has a superb Web site. This kind of one-stop shopping is also offered through emerging Federal sites, such as seniors.gov, students.gov, fedstats.gov and many others.

These sites illustrate the value of real customer focus, but they also demonstrate, in the way that they are managed the challenges of real cross-agency interaction. An important role for a Federal CIO will be to lead in defining these areas of customer focus and in forging partnerships among agencies to enable better targeting

of services. These are aggregations of services that go beyond a simple bundling of the stovepipes that we've been talking about.

The second challenge is the rapid evolution of technology. Moore's law shows no signs of being repealed. Software is becoming the principal building material for competitive advantage in many sectors, ranging from health care to banking and other sectors.

As you know, the Federal Government has a principal role in long-term innovation in information technology starting as early as the 1890 census with Hollerith's punched cards. I am presently chairing a National Research Council committee that is looking at advanced information technology in government. We've issued two reports on crisis management and Federal statistics identifying a number of long term technical challenges. We are completing a final report that is more broadly focused and that addresses some of the issues that we are considering today.

Mission agencies with organic research capability have developed a culture of IT innovation to help ensure that their special needs are addressed over the long term and also that they can respond rapidly to new challenges, for example, in the security area. A Federal CIO could help create this culture of innovation throughout the government.

A third challenge is the overall mechanism by which we undertake and manage IT acquisitions. Consider the case of a major Internet portal—commercial or governmental: Requirements are unlikely to be fully clear at the outset. The underlying technologies are evolving rapidly. And the capability, once we deliver it, will need to continue evolving rapidly. The security environment, for example, is complex and continually changing.

Although I am not an expert in acquisition processes and regulations, it is clear that the present mechanisms and culture remain oriented around what is called the waterfall model. This model is not well-adapted to experimentation or prototyping or other forms of focused, careful risk-taking. Program managers often seem to resist the use of more aggressive acquisition models including those already available in the Clinger-Cohen Act; for example, modular acquisition and the use of commercial off-the-shelf components. Why? Because they have strong incentives to meet schedules and costs—to make these as predictable as possible and risk at a minimum—even when it comes at a cost of overall capability, flexibility, interoperability, and other less easily measured attributes.

The Federal CIO should have a major role in helping agency CIOs structure incentives—and regulations where appropriate—to facilitate risk-managed acquisition processes.

My written testimony addresses several other areas where this Federal CIO could provide this positive leadership.

I would like to conclude by saying that I support the concept of a Federal CIO who can provide this positive leadership and who can catalyze effective—and pervasive—government response to both the challenges and the opportunities of delivering government online. Thank you very much.

Mr. HORN. Thank you very much.

We appreciate—I would like to have a definition before we leave you of the waterfall concept. Is that when you put somebody in the barrel, and they go over Niagara Falls? Just so we can get bureauc-

racy cleared up today because we will have two asterisks that I've gained. So I do not regard this as something I have cared not to do. I am very interested in doing it, and you have all been memorable. So it will be the Scherlis law and the Flyzik law.

Tell me about the waterfall.

Mr. SCHERLIS. The waterfall model is a term that refers to a traditional step-by-step acquisition model. First a process is undertaken to initially formulate a precise definition of the system requirements. This is a process that sometimes can take years. After this is complete, then contracts are let and development processes are undertaken, followed by test and evaluation and ultimately delivery. But by the time the capability is delivered, the world has evolved and the requirements have changed, even assuming they were correctly identified at the outset.

That's the waterfall model. It is a model that works well only for classes of systems that we have already developed successfully. It does not work well for systems that have even mildly innovative character.

Mr. HORN. Having spent part of my life for 22 years at one university, I now think that even the Federal Government looks efficient. But I think you would agree on that. Things take a lot longer in the university. OK.

Our last presenter and one individual who is very well known to this committee, and we appreciate all he's done for this subcommittee over the last 5 to 6 years, Dwight Ink is President Emeritus of the Institute of Public Administration. He was a former Assistant Director for Executive Management in the Office of Management and Budget from 1969 to 1973. A highly respected civil servant, he was taken by various Presidents to clean up this agency and that agency and another one.

So we welcome your thoughts, Mr. Ink. You've got—I will give you 6 minutes.

STATEMENT OF DWIGHT INK, PRESIDENT EMERITUS, INSTITUTE OF PUBLIC ADMINISTRATION, FORMER ASSISTANT DIRECTOR FOR EXECUTIVE MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET (1969-1973)

Mr. INK. Thank you, Mr. Chairman, Mr. Turner and Mr. Davis. It's a pleasure to be here. By the way, I didn't think the waterfall approach ever worked very well.

In summary, I believe the sponsors of these bills are correct in searching for ways in which to strengthen the information technology leadership capacity of our government. I do not believe these bills, however, provide the best way of achieving those goals, and, in fact, I think they may weaken what the sponsors are trying to accomplish. I would also urge that the committee look at this issue as well as others from the total Presidential perspective and the total congressional perspective rather than just IT. Otherwise I think we contribute to further growth of a stovepipe approach to government.

First, as was said at the beginning of these hearings, IT certainly should be regarded as an integral part of the agency administrative and program activities. It is really the glue that connects everything else people do in government. So one of our goals, it seems

to me, should be to search for ways to better integrate information technology with other management and program activities.

I believe establishing a Federal Chief Information Officer that is freestanding and separate from other elements of management leadership will work against the need for integration.

I also have some questions about the feasibility of some of the separation that is contemplated. For example, there are several paperwork reduction functions that are transferred out of OMB to this new office, and yet the basic tools for dealing with red-tape-cutting remain in OMB. So if these bills are passed, the leadership for cutting red tape is divided between two agencies, and I think that tends to result in nibbling at problems rather than reforming government processes.

I think that fragmenting central management responsibilities inevitably creates unnecessary burdens for the agencies. Again, this is part of your stovepipe problem that was mentioned earlier.

I believe this separation not only weakens IT over the long haul, it weakens other management functions. In my view, the more we establish organizational barriers among different fields of management, the less one area will benefit from the other, the less synergistic value we gain, and the more we handicap the President and the agencies in modernizing government.

I would also ask the question if it should be regarded as necessary to have a freestanding IT unit in the Executive Office of the President, should we not do the same with respect to financial management, an extremely important area? What about procurement? What about program management? Everyone wants to be independent and report to the President, but in my view, this is the road to confusion, higher cost, managerial chaos and, again, stovepipe government.

I do not see the freestanding IT office as having the capacity to provide the strong leadership that I know Mr. Davis, and Mr. Turner are seeking. People tend to assume that any office that reports directly to the President, especially if they are within the Executive Office of the President, has muscle, but this is simply not true. I know. I've been there.

In fact, it is difficult for any organization to gain sustained attention on management issues because there are so many competing pressures within the Executive Office of the President. The OMB uses the leverage of the budget to help on issues directly related to the budget, but other management issues have great difficulty in competing with the budget pressures in OMB. A freestanding IT would have not even the budget leverage.

In discussions about a separate Office of Management which have taken place in this committee, we've listed a series of elements of that office which we believe are absolutely necessary to provide the leverage needed to provide effective leadership on behalf of the President. I don't see any of those levers present in this separate IT. Without these levers, an Office of Management, I think, would not be wise, strongly as I support the concept. I believe a more narrowly based, freestanding IT would be even more impotent. Even with a structure separating these two, there would have to be some relationship to OMB. But who would coordinate IT and OMB? I mentioned other problems in my testimony.

Although I do not support a freestanding IT, I do agree with the sponsors that it is desirable and, very important to take steps to enhance the IT leadership structure. This is one of the reasons I support the Office of Management which has been under consideration by this committee. The OMB leadership is hard pressed by complex annual budget and economic issues, and its leadership simply does not have the time to provide the focus and the energy that IT leadership requires in this day and age. An Office of Management would provide this leadership focus. It would provide the integration, and avoid the fragmentation of an isolated IT office.

In summary, I believe an Office of Management, given the necessary leverage, would be a much better solution to what I agree is a need for greater IT leadership capacity. It would have the leverage and avoid isolating IT from other components of management leadership. Though I think these bills would have unfortunate unintended consequences that would run counter to the intent of the sponsors, I do agree with the sponsors on the need for change. I just think there's a better way to achieve their objective. Thank you.

Mr. HORN. Thank you very much.

[The prepared statement of Mr. Ink follows:]

STATEMENT OF DWIGHT INK
President Emeritus, Institute of Public Administration

Before the

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND
TECHNOLOGY

HEARING ON INFORMATION TECHNOLOGY
September 12, 2000

Statement of Dwight Ink
September 12, 2000

Mr. Chairman and Members of the Subcommittee:

I am pleased to have the opportunity to share my views on the basic organization concepts contained in two bills, H.R. 5024 and H.R. 4670.

To summarize, I believe the sponsors of these bills are correct in searching for ways in which to strengthen our Information Technology (IT) efforts to improve government. However, I believe these bills do not provide a good way of achieving their goals. In fact, over the long period I fear they would weaken what the sponsors hope to achieve. I would also urge the Committee to look at this issue from the total presidential and congressional perspective of government operations, not just IT, important as that is. There are several reasons for this view.

Integration. First, IT is an integral part of agency administrative and program activities. It is a fundamental part of financial management, it is a part of procurement, and it is an essential part of project management. In many respects, it is the glue that connects everything else people do in government. One of our goals should be to increase the awareness of people to that fact and search for ways to integrate modern IT with their day-to-day work. Establishing some version of a Federal Chief Information Officer that is free standing and separate from other elements of management leadership that are now located in the Office of Management and Budget will work against this need for integration.

I also have serious doubts that some of the separation contemplated, even if desirable, is feasible. H.R. 5024, for example, transfers to a CIO several functions relating to paperwork elimination and reduction. Others are necessarily left in OMB. As a result, leadership for cutting red tape would be divided between two agencies, making it very

difficult to launch broad based attacks on costly paperwork. I believe this splitting of leadership would tend to result in nibbling at burdensome government processes rather than reforming them.

I would also suggest that fragmenting central management responsibilities inevitably creates unnecessary burdens for the agencies. The agencies may try to coordinate diverse initiatives emerging from different pieces of the EOP, yet they rarely have the muscle to do so. Monitoring of agency performance becomes more complex, and my experience would suggest that it is likely to become more vulnerable to gaps in information gathering and early warning of problems involving different disciplines.

Not only would the level of separation from other elements of management contemplated by these bills lead over time to a weakening of IT, I believe it would weaken the other management functions that need to build the latest information technology into their programs. The more we set up organizational barriers among different fields of management, the less one area will benefit from the others, the less synergistic value we gain, and the more we handicap the president and the agencies in modernizing government.

Fragmentation. If it should be regarded as necessary to have a free standing IT unit reporting to the President, should we not do the same with respect to procurement, financial management, etc? Everyone wants to be independent and report to the President, but that is the road to confusion, higher costs, and managerial chaos.

Leverage. I do not believe a free standing IT office would have the capacity to provide strong leadership over the long term. People tend to assume that any office that reports directly to the President, especially if located in the Executive Office of the President (EOP), has muscle. This is simply not true. In fact, it is difficult for any organization to gain sustained attention on management issues, because there are so many competing pressures in the EOP.

The OMB uses the leverage of the budget to help on issues directly related to the budget, but other management issues have great difficulty competing with the budget pressures. A free standing IT would not even have the budget leverage. In advocating a separate Office of Management, several have listed a series of elements of that office believed to be necessary to provide the leverage needed to provide effective leadership on behalf of the President. These include the development of presidential executive orders, issuance of regulations covering a broad range of subject matter, legislative clearance, and leadership for inter-agency and intergovernmental management issues. It was these types of leverages that enabled an earlier Office of Executive Management to have a seat at the White House daily 7:30 meetings and to inject management considerations into critical presidential issues as they were developing. Without these levers an Office of Management would be largely ignored. I believe a more narrowly based free standing IT office would be even more impotent after the initial fanfare had faded into the background. I do not see the levers that would give it a seat at the table.

Coordination. Even though I do not see the structural separation permitting the integration among the fields of management I regard as important, there would nevertheless have to be some degree of coordination with OMB. But who will provide it? Who will settle disagreements between the two? If the answer is OMB, then the IT will be irrelevant and scarcely noticed. Despite reporting to the President, a separate IT will not have the strength.

The White House and the EOP are already too cluttered in the opinion of most close observers. Clutter tends to dilute accountability and creates confusion. It makes life difficult for departments and agencies. We ought not to go further down that road without a compelling reason.

A Different Solution. Although I do not support a free standing IT, I agree with the sponsors that it is desirable to take steps to enhance the IT leadership structure. In fact, this is one of the reasons I support the Office of Management, which has been under consideration by this Committee the last several years.

The OMB leadership is understandably hard-pressed by complex annual budget and economic issues. It has had increasing difficulty in devoting the time and resources required to address questions of long term IT and capital improvement investments, crosscutting management problems, major agency and interagency structural problems, intergovernmental and interagency coordination, or program operation concepts that involve every component of management.

I believe an Office of Management, given the necessary levers, would be a much better solution to the need for greater IT leadership capacity.

In summary, I believe these two bills would have unfortunate unintended consequences that would run counter to the intent of the sponsors. Yet I agree with the sponsors on the need for change. I think there is a much better way to reach their objective.

I would be happy to respond to questions.

Mr. HORN. That's very helpful testimony, and I can tell you've—given the preciseness within your paper, that you've spent a lot of your life on trying to get to the essence of a problem. So we're grateful that you've come from various States where you're now living and giving us some wisdom. So we thank you.

We now have the questioning. The gentleman from Texas Mr. Turner, 5 minutes for questioning, and then Mr. Davis.

Mr. TURNER. Thank you, Mr. Chairman.

We appreciate the testimony that each of you has given us, and I think it is apparent to us that every witness on the panel, perhaps with the exception of Ms. Katzen and Mr. Ink, have advocated a Federal CIO. We all respect that there is a clear issue we must correctly address as to how it should be structured.

That is not to say that we should not address it within the context of the remarks Mr. Ink made. And I know Mr. Ink has been an advocate of separating the Office of Management and Budget into two entities with a Director of the Budget and a Director of Management, but it does seem that at least as we look to the private sector, the private sector has recognized the importance of having a chief CIO who works with the CEO and the CFO.

I might ask, Mr. Scherlis, if you wouldn't mind commenting on the CIO in the context of the remarks Mr. Ink made as to where you think the structure should be in order to perhaps accommodate the kind of concerns that we just heard expressed from Mr. Ink, who definitely has a vast experience in the Federal Government.

Mr. SCHERLIS. I enjoyed and appreciate his remarks, but I am unfortunately not familiar with the recommendations that were voiced here earlier concerning the concept of a separate Office of Management. But pertinent to the issue is the recent report released by the President's IT Advisory Committee on August 31 concerning transforming the government through information technology. It recommends creation of a new office within OMB called the Office for Electronic Government [OEG], with strong senior leadership. Although the concept of the Federal CIO is not explicit, the recommendations that we're talking about today are consistent with the recommendations of that report.

The reason for separating the OEG from the OIRA within OMB is to create a focus of positive leadership that is separate from regulation and policy. There are many roles that are now being bundled together in one organization, and some separation of those roles is appropriate.

On the basis of comments of Mr. Ink today, I believe that the recommendations that I've voiced are consistent with his comments.

Mr. TURNER. Mr. Atkinson, do you have an observation here?

Mr. ATKINSON. Yes, The major point I would want to stress after listening to Mr. Ink's comments is that information technology is fundamentally different. This is to me the central mission, the central challenge facing the Federal Government today, and it will be the central challenge for this decade, just as when we made this last major transformation from an old economy to a new economy back in the 1930's and 1940's, and we created all new management structures in the Federal Government. I think this is just as equally a major transformation. This is about creating a fundamentally

new economy, a digital economy, and it's creating a fundamentally new type of government.

And I don't think that the existing structure of OMB or even in the Office of Management is suited to do that because the key to all of this is digital reinvention, and I think the core of that has got to be someone who is a CIO, who has that as their sole mission.

The second point would be I think Mr. Ink mentioned we need to think beyond IT. I couldn't agree more. We need think beyond IT. That's why I think the CIO—if the CIO is just a glorified computer systems manager, then we won't think beyond IT. But if you think where the States are, most of the States' CIOs, when you listen to what they have to say, they're the ones that are arguing—all their language is about cross-cutting applications, breaking down barriers between bureaucracies and agencies who don't want to do that. And I think that's why the CIO is central to making all this happen.

Mr. TURNER. Mr. Rummell, I would like to hear your comments on it. I heard you say at the beginning of your testimony you've been working in the IT field for 30 years. One of the things I see lacking today in OMB is anyone with the background, the experience, the expertise to really move us forward aggressively in IT, but perhaps you would have some comments to share on the subject?

Mr. RUMMELL. First of all, when I started with the Federal Government of Canada, I went on a whistle-stop tour of the departments and talked to the heads of the departments and agencies and the heads of the technology function of the departments. And I asked them what they were looking for from me as the new CIO for the government, and they said to me, leadership. And that surprised me, being in the land of leaders, because I suspected that all these people were leaders by themselves, but they really were looking for my leadership.

They also were looking for us to provide the strategic direction; that was an overall context to take it from a 50,000-foot elevation right down to ground level, and provide direction with large projects that were in trouble, to provide for e-government initiatives to coordinate and deliver services, and from the things that we put into place, we made a lot of progress. There was a lot of frustration. We really provided focus, and I think we provided a very solid operational plan, and I think that's what I was able to accomplish is that focal point.

Mr. TURNER. Thank you.

Mr. McClure, when you look at the existing structure of OMB, is there anyone there who by education or background is uniquely qualified to fill this role today or—and I guess I might ask you is there anyone over there who has that as their sole responsibility?

Mr. MCCLURE. No. I think that highlights the concerns that I raised in my testimony, Mr. Turner. The Deputy Director for Management created by the CFO Act wears many, many hats, both the Chief Financial Officer, general management functions, statistical policy, procurement. The list is quite long in terms of overall management responsibilities of the Deputy Director for Management.

Similarly in OIRA, the OIRA Administrator is really focused heavily in terms of resources on information collection requests, on

burden reduction reviews and on calculating the cost and benefits from Federal regulations. So a lot of the staff in OIRA are focussed on these issues as opposed to the IRM or IT issues. So as a result we don't have someone in OMB full time focused, I would argue, on some of these important IT issues.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. The gentleman from Virginia Mr. Davis.

Mr. DAVIS. Thank you. I also want to extend my thanks to all the panelists.

Mr. McClure, let me go back and ask you a question that I asked Ms. Katzen earlier. I asked if she could describe the leadership role that OMB has displayed in the past in defining—in managing interagency items. I am not just speaking of money items, but managing IT resources. How do you think OMB has kept track of those initiatives so that responsive decisions could be made when projects aren't working and should be halted or when a new direction should be taken?

Mr. McCLURE. Mr. Davis, I think since the passage of Clinger-Cohen, to its credit OMB has certainly stepped up to the plate with some specific guidance, better guidance in many areas, for the agencies, in architecture, investment control, capital planning. We've worked actually with OMB in revising some of the guidance. I think the question for OMB is how to use the information that results from that new guidance to make really tough decisions about stopping, delaying, canceling or even accelerating good Federal IT programs, and that, I think, is where the jury is out.

The fortitude of OMB to be able to step up to the plate and stop projects has not always been clearly demonstrated, in our opinion.

Mr. DAVIS. Mr. Flyzik, let me ask you a question. Can you give me any recommendations that have been made by the CIO Council that have been implemented by OMB?

Mr. FLYZIK. What OMB has been doing with us, sir, is working to facilitate our recommendations. We do have a whole list of things that we have moved on, and moved quite quickly on. We have a whole lineup of interagency activities. The FirstGov project comes to mind; our public key infrastructure in the bridge certificate authority that enables digital signatures to really happen; the Access America series, Access America for seniors and students. We have a number of wireless initiatives. We have the Federal Commons Project, the Enterprise Project. They are supporting us on the concept of ITPS, or the information technology portfolio system, which will give us a common platform for building IT portfolios across government.

The OMB role has evolved to one that I think has been working well. In the beginning, I guess, the Council went through kind of a bonding process, trying to figure out who we are and what we're going to do. I think we've moved over time into more of a leadership role where OMB is giving us support to move forward on projects and is listening and working with us.

Mr. DAVIS. So as far as information resources management goes, you think that OMB is handling this, this statutory authority, is handling it well?

Mr. FLYZIK. I think it's evolving well under the guise of Clinger-Cohen. I do believe we're moving in a very, very positive direction. OMB is supporting us.

As you're well aware, the Council does not have authority to issue policy. OMB does. What we do is we've been working with OMB in situations where we need policy guidance.

Mr. DAVIS. Right. But can you give me a specific recommendation that you've made to them?

Mr. FLYZIK. We have Internet use policy. We're working on privacy policy now. We have a dialog ongoing on our Internet privacy issues and a number of things along those lines.

Mr. DAVIS. Mr. McClure, do you have any observations on that?

Mr. MCCLURE. I think, as I said earlier, I agree with Mr. Flyzik that the role of OMB has changed under the recent passage of laws. They had tremendous responsibilities for not only issuing guidance, but also oversight responsibilities for major IT projects in the Federal Government. So, again, I return to the point, OMB should not be totally focused on justification for projects in the Federal budget. It also should play a role in stepping up and helping control projects that are out of line in terms of cost, schedule and performance.

And in that area, again, I think that the track record is not what we would like to see it to be.

Mr. DAVIS. Mr. Doll, let me ask you a question: In States where the CIO has multiple bosses, reports to one or more cabinet secretaries, what's their experience in achieving an integrated and coordinated information resources management policy?

Mr. DOLL. Where States' CIOs deal with multiple entities to get the job done, because of the typically high level, whether it's to the Governor's staff in addition to some council, or other entity that controls, again, it's a statewide implementation and application of technology across the State. And I think that's truly what the key is, because unless they're inserted at a level in the organization that's looking at IT as an entity in a field that helps make vision reality, then that's where they can have impact.

Most States have put IT up there with human resources, financial management, administration, services that are used to make the vision of a Governor happen. And whether that is put through some committee or some special commission that a Governor has established or to the Governor directly, it's really that orientation of saying that to make the vision of education, whether that may be in a State or make the vision of economic development happen, that what you're trying to do is align this information technology world to see that as a reality.

Mr. DAVIS. Mr. Atkinson, let me ask you a question: You make a strong case for the need for a strong centralized leader to achieve a digital Federal Government. What, in your opinion, are the flaws in current structure placing IRM responsibilities with OMB? Ms. Katzen seems to conclude that instead of a Federal CIO, OMB should have a strengthened role. How do you respond to that?

Mr. ATKINSON. Well, I think a major reason I would say that, is that I don't think that would achieve what you all are wanting to achieve and others are wanting to achieve. OMB is responsible, as Mr. McClure mentioned, for so many other things. And I don't

think it would give the leadership that, for example, Ms. Katzen provided on the Y2K issue where it is much broader than that. Let me just mention another example. A lot of what I think digital government is about frankly is the details. And let me just mention one—Students.Gov—which is a portal for students. It's a very good effort, it's a great effort, and the people who developed it should be commended. The problem is with Students.Gov, though, it's what other agencies are doing. For example, in the Department of Education, they have their own Web site designed around students. On Students.Gov, you can apply for a student loan online. On the Department of Education Web site, you can't apply for a student loan online. There's no link back to Students.Gov.

I can give you many more examples like that. What I think they're a reflection of is agencies doing their own thing. Even when they can get together with a portal like Students.Gov, you still have agencies doing their own thing. That's why it requires centralized leadership—will drill down into that level of detail to make it a much more coordinated system.

Mr. DAVIS. Thank you very much. Mr. Chairman, I yield back and thank the panel for their indulgence.

Mr. HORN. I thank the gentleman. And I don't believe the gentleman from Texas has any more questions. I have just one or two. And Mr. McClure, I don't want to put you on the hot seat, but the question is this: Of the two bills being considered, which one is closest to what you would consider to be a Federal chief information officer's role, responsibilities and empowerment as far as GAO feels is their recommendation?

Mr. MCCLURE. The seat is very hot, Mr. Chairman. Especially with both members present.

Mr. HORN. I don't know how it's going to come out either, but I thought we'd like your views on it. But you did a great report there.

Mr. DAVIS. We're not taking names.

Mr. MCCLURE. I just want to reiterate that both of them have positive characteristics. There's no reason why things that are in both bills could not ultimately be combined or considered together. I think the real question is whether this position is inside or outside of OMB. That seems to be the drawing distinction. There are clear advantages for having the CIO outside of OMB and contained within the executive branch. Because of many of the reasons that we went over today, it avoids the problem of multi-hatted responsibilities within the Office of Management and Budget.

Having said that, it also creates, as many people have said, tremendous risk in that you're removing that budget lever from the chief information officer. I don't think that's necessarily true and it's certainly not true in private sector and public sector CIOs who do not have budget control either. They simply have to come to the table and work with those individuals that have budget control and the two combined can pull that lever.

And I think that's the attraction that these bills have is they free up time for somebody to focus full time on such issues like electronic government and security at a time desperately where we need that kind of attention. It also allows them to sit at the table

with the Director of OMB and have some very frank input on some budget directions and budget control.

So I think, again, I've avoided answering directly, but I think that's the positives that I see in both bills.

Mr. HORN. Mr. Doll, if I might, let me try this question out on you, and you probably don't have the answer, but maybe you do. A number of Governors change every once in a while based on the election. Have you found that the chief information officer of a State is carried on by another Governor, or do they have to sort of be partisan in relation to the Governor? What's your sort of off-the-top-of-the-head view of that.

Mr. DOLL. Well, to give you a scope, we've lost 16 CIOs this calendar year for one reason or another. Most going to the private sector. A number of those tied to the fact that this is the last year of the Governor's term. So we expect in the future that you will get this turn over. I think it's critical that the CIO be aligned to the Governor so that his or her vision can be carried out. And not someone who as you mentioned, will be able to sort of pass from administration to administration. Yes there is value in that, but the rest of the civil service below that level is typically there year after year, term after term. The key part to us at least in talking with my colleagues is making vision reality and applying information technology to that. And you have to be close and have the same orientation as that Governor to be successful in my mind.

Mr. HORN. Mr. Rummell, I really have the same question in relation to the Canadian Government. When there were turnovers, did the CIOs in the agencies change or what?

Mr. RUMMELL. There have been changes, again we've kept the same government so there haven't been political changes. There certainly have been no new CIOs appointed or rotated based upon the changes in the heads of agencies. I guess one of the other things that we had too, if I could make another comment, that was a terrific feature started in our government was agency heads would meet at a committee on information technology issues. They took a role of very active sponsorship and met at least once a month for 1 to 2 hours, and discussed cross-cutting IT initiatives across the agencies and departments and the Canadian Government, and that really raised the level of sponsorship for the CIOs and for initiatives that were providing overall services to the public. So that's where I think we were also able to make a difference. Thank you.

Mr. HORN. Well, thank you. I want to thank this panel.

Mr. INK. Mr. Chairman, could I make one rebuttal comment?

Mr. HORN. OK.

Mr. INK. I think the States provide excellent ideas, excellent examples in many areas of governmental activity. You look at welfare reform, for example, they were well ahead of the Federal Government. And I think in terms of information technology, as it relates to the delivery services, States have a lot to offer. But I wanted to tell you there is a tremendous difference between operations within a Governor's office and that within the President's office. The leap in terms of pressures and the difficulty of having a workable base which will provide the strength for leadership is entirely different. Look at the West Wing program. I was thinking yesterday about

the daily meetings I used to participate in with the top White House staff. Had I had responsibilities for only information technology or only procurement or only financial management, I wouldn't have been there, much less have had a voice at the table. Separate IT isolated from these other responsibilities will not have a voice at the table. Much as people might wish it otherwise, I think that's the fact of life, that's the way the President's office functions.

Mr. HORN. Well, we thank you for that. We thank you also for coming on less than 24 hours' notice. And——

Mr. INK. Much less.

Mr. HORN. Much less. I think all of your testimony has been very helpful and I'm grateful to you. I think some of the charts all of you provided was also very helpful. Staff on both sides might wish to have some questions sent out to you, and if you would take some time and give us a couple of answers, we'd like to put them at this point in the records if there's some we've missed or there's something you'd like to get on the record.

But right now I'm going to thank our staff who put all this together: J. Russell George, staff director, chief council of the subcommittee; gentleman to my left, your right is Randy Kaplan, council to the committee, and he's worked on this particular hearing; and yesterday Ben Ritt, professional staff member on loan to us from the General Accounting Office, which always has good people and we're glad to use them; Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong, staff assistant; George Fraser, intern; and from Mr. Turner's staff, Trey Henderson counsel, he's on his right; and Jean Gosa, minority clerk. And Mr. Davis' staff, Amy Heerink, we know how good she is on a lot of these things, and Melissa Wojciak. Then our court reporters are Julie Thomas and Colleen Lynch, and we thank you very much. And we adjourn the meeting.

[Whereupon, at 12:16 p.m., the subcommittee was adjourned.]

