United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs,
U.S. Senate

For Release
Expected at
9:30 a.m. EDT
Wednesday,
July 11, 2001

ELECTRONIC GOVERNMENT

Challenges Must Be Addressed With Effective Leadership and Management

Statement for the Record by David L. McClure
Director, Information Technology Management Issues

G A O
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to participate in the Committee's hearing on electronic government (e-government) issues and S. 803, the *E-Government Act of 2001*. Advances in the use of information technology (IT) and the Internet are continuing to change the way federal agencies communicate, use and disseminate information, deliver services, and conduct business. It has the potential to help build better relationships between government and the public by facilitating timely and efficient interaction with citizens. According to a January 2001 poll, nearly half of Americans have used a government Web site and almost three-quarters believe that e-government should be a high priority.[1]

Generally speaking, electronic government refers to the use of technology, particularly Web-based Internet applications, to enhance the access to and delivery of government information and service to citizens, business partners, employees, other agencies, and entities. At the federal level, agencies have identified 1,371 electronic government initiatives, ranging from those that simply disseminate information to those that are expected to transform the way the government operates. With respect to states, according to the National Association of State Chief Information Officers, government-to-business electronic interaction is well underway and government-to-citizen and government-to-government electronic interaction is rapidly increasing. At the local level, a survey in the fall of 2000 by the International City/County Management Association and Public Technology, Inc. found that about 83 percent of local governments had a Web site but that few local governments were providing interactive service delivery[2] on line, although many jurisdictions plan to offer such services.

While the Internet opens new opportunities for streamlining processes and enhancing delivery of services, federal executives and managers must also be cognizant of the responsibilities and challenges that accompany these opportunities. These challenges include (1) sustaining committed executive leadership, (2) building effective e-government business cases, (3) maintaining a citizen focus, (4) protecting personal privacy, (5) implementing appropriate security controls, (6) maintaining electronic

[1] Hart-Teeter poll reported in *e-government: The Next American Revolution* (The Council for Excellence in Government, February 2001). This was a nationally representative survey among 1,017 American adults for the Council conducted January 4-6, 2001. The survey findings have a margin of error of 3.1 percent.

[2] The survey defined interactive service delivery as two-way communications in which a Web site visitor can submit information or payment, as well as receive information.

records, (7) maintaining a robust technical infrastructure, (8) addressing IT human capital concerns, and (9) ensuring uniform service to the public.

Strong and focused central leadership could help overcome these challenges. A federal Chief Information Officer (CIO) could provide such leadership. We have long supported the establishment of a federal CIO to provide the leadership needed to address the major IT issues facing government, including those related to e-government and security. S.803 calls for the establishment of a federal CIO, who would report to the Director of the Office of Management and Budget (OMB) and would be responsible for a variety of information technology and management functions.

In my remarks today, I will (1) provide an overview of the status of federal e-government initiatives, (2) describe the key challenges the government faces in implementing its e-government initiatives, and (3) discuss the federal CIO approach proposed by S. 803, the *E-Government Act of 2001*. To provide additional information on our e-government work, I have also included, as an attachment, a list of pertinent GAO publications on e-government issues.[3]

Status of Federal E-government

As we testified in May 2000, the public sector is increasingly turning to the Internet to conduct paperless acquisitions, provide interactive electronic services to the public, and tailor or personalize information.[4] In particular, federal agencies have implemented an array of e-government applications, including using the Internet to collect and disseminate information and forms, buy and pay for goods and services, submit bids and proposals, and apply for licenses, grants, and benefits. The reach of e-government extends not just to citizens and the various communities of interest that represent them but to many other constituencies as well.

A recent evaluation of 22 countries' e-government development by Accenture—a private-sector management and technology consulting firm—found that the U.S. federal government was one of three "innovative leaders"[5] that stood apart from other countries due to the high number of

[3] These publications can be obtained through GAO's World Wide Web page at *www.gao.gov*.

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

[5] The other countries designated as innovative leaders were Canada and Singapore.

mature services offered online.[6] Accenture found that the federal government excelled in service maturity breadth, the level to which a government had developed on-line presence. However, according to the report, "the focus on building the volume of services and individual agency online sophistication has clearly not allowed time for agencies or the Federal Government to focus on incorporating … [best practice] techniques." Accordingly, the U.S. government was deemed below average in delivery maturity, which indicates the sophistication of delivery mechanisms, such as a single point of entry and customer relationship management techniques.[7]

Status of Agency GPEA Implementation

The Government Paperwork Elimination Act (GPEA)[8] requires that by October 21, 2003 federal agencies provide the public, when practicable, the option of submitting, maintaining, and disclosing required information electronically. The act makes OMB responsible for ensuring that federal agencies meet the act's implementation deadline. OMB, in turn, required each agency, by October 2000, to develop and submit an implementation plan and schedule.

In recent testimony on the implementation of GPEA, the Director of OMB stated that "agency progress in going electronic is mixed."[9] Specifically, he stated that upon evaluating specific agency plans for compliance with the act, OMB found that some agencies were not prepared. According to OMB, the Departments of Defense, Health and Human Services, and Justice submitted plans that indicated that they have not fully adopted the goals of GPEA and do not have an agencywide commitment to moving into the electronic arena. In contrast, OMB cited the Departments of Housing and Urban Development and the Treasury and the Environmental Protection Agency as having developed solid plans for meeting the act's objectives.

[6] *eGovernment Leadership: Rhetoric vs Reality – Closing the Gap* (Accenture, April 2001). Accenture carried out its research in January 2001. It surveyed 165 national government services in nine major sectors—human services, justice and public safety, revenue, defense, education, administration, transport, regulation and democracy, and postal. Services were categorized into three levels of service: publish, interact, and transact. Within each level, services were scored to show the maturity that they had reached.

[7] Accenture's evaluation of the service and delivery maturity of each government were combined into an overall maturity level. In calculating the overall maturity level, Accenture assigned a weight of 70 percent and 30 percent to the service and delivery maturity levels, respectively.

[8] P.L. 105-277, Div. C, tit.XVII.

[9] Statement of Mitchell E. Daniels, Jr., Director, OMB ,before the House Committee on Government Reform, June 21, 2001.

Mr. Chairman, as you know, we are currently conducting a review of agency GPEA implementation plans at your request. While not complete, our work has found that, taken in isolation, agency GPEA plans do not provide sufficient information to assess agencies' progress in meeting the objectives of the act.[10] Specifically, the plans do not provide sufficient information with which to assess whether agencies have been engaging in critical activities such as (1) examining business processes that might be revamped to employ electronic documents, forms, or transactions, (2) identifying customer needs and demands as well as the existing risks associated with fraud, error, or misuse, and (3) evaluating electronic signature alternatives, including risks, costs, and practicality.

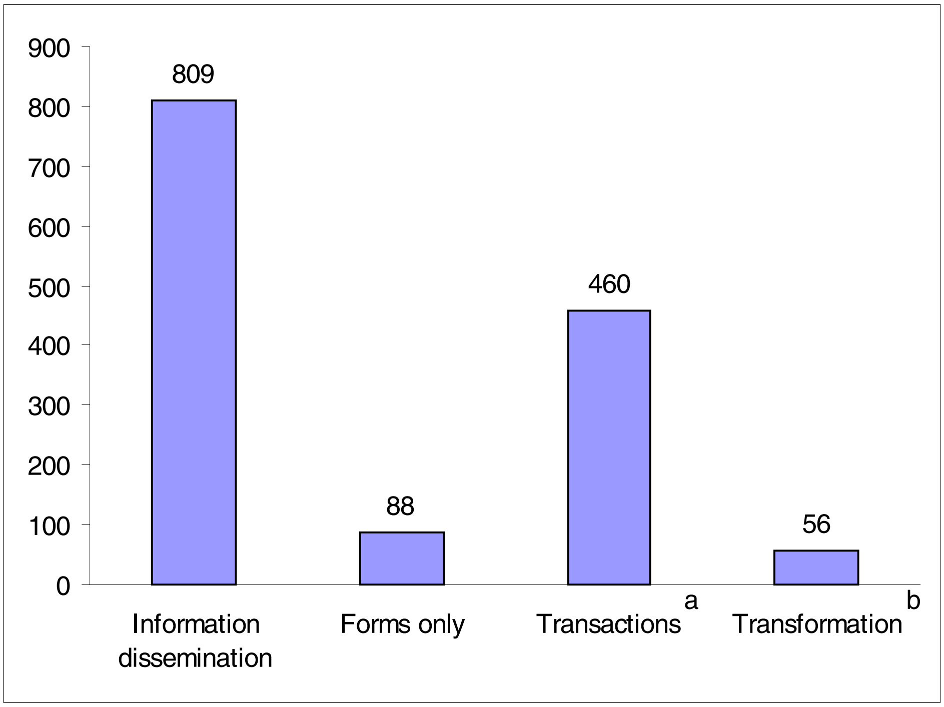
Agency E-government Initiatives

Federal agencies have implemented, or are in the process of implementing a wide variety of e-government initiatives. This variety is illustrated by chart 1, which depicts the types of federal e-government initiatives reported by 37 departments and agencies. The category[11] with the greatest number of initiatives is "information dissemination"—reported by the General Services Administration and the federal CIO Council to be the least technically complex; it involves implementing applications on the Internet that make electronic information readily accessible. In the next category—"forms"—agencies provide downloadable electronic forms. The "transaction" category is a more complex implementation of e-government and includes initiatives such as submitting patent applications via the Internet. Finally, in the last category—"transformation"—the e-government initiative is expected to transform the way the government operates. For example, the Navy's Virtual Naval Hospital initiative provides a digital science library, and is designed to deliver expert medical information to providers and patients at the point of care.

[10] *Electronic Government: Selected Agency Plans for Implementing the Government Paperwork Elimination Act* (GAO-01-861T, June 21, 2001).

[11] The report characterized these categories as the four phases of e-government based on a Gartner (a private research firm) model that demonstrates the progression of e-government.

Chart 1: Types of Federal E-government Initiatives



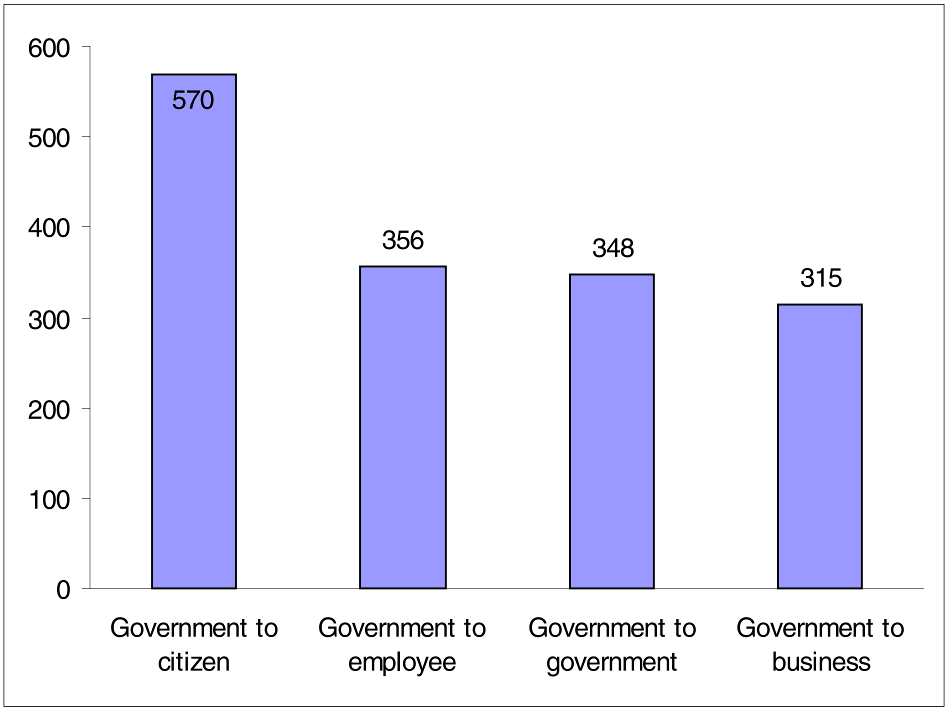
[a] Defined as end-to-end transactions completed electronically.
[b] Defined as initiatives in which the government has taken a global focus, government involvement is minimized, and citizens do not have to know the government organization to obtain the services needed.

Note: In some cases an agency listed the same initiative under more than one type. The total number of unique initiatives reported was 1,371.

Source: *An Inventory of Federal e-Government Initiatives* (General Services Administration in cooperation with the federal CIO Council, January 2001).

Chart 2 shows the constituencies that the e-government initiatives are targeting, with the greatest number serving the citizen.

Chart 2: Categories of Constituencies of Federal E-government Initiatives



Note: In some cases an agency listed the same initiative under more than one constituency category. The total number of unique initiatives reported was 1,371.

Source: *An Inventory of Federal e-Government Initiatives* (General Services Administration in cooperation with the federal CIO Council, January 2001).

For each type of constituency, let me briefly describe a few major e-government projects that agencies have implemented or plan to implement:[12]

- *Government-to-Citizen.* One of the major benefits of on-line and Internet-based services is that they provide opportunities for greater

[12] We have not performed an independent evaluation of these initiatives.

citizen access to, and interaction with, the federal government. Initiatives such as *Access America* provide Internet access and services organized to meet the needs of specific communities of interest. As part of this initiative, over 40 federal agencies have been working together on Web portals that provide information, news, and some capabilities for on line interactions with federal agencies and programs that serve the target groups. For example, *Access America for Seniors*—also called *FirstGov for Seniors*— is designed to be an entry portal for senior citizens to reach government services and information on such topics as benefits, taxes, health and nutrition, and consumer protection.[13] In another example, the Department of the Treasury's Bureau of Public Debt has partnered with Treasury's Financial Management Service, Mellon Bank, MasterCard, and IBM to build an Internet-based system—*Savings Bond Direct*—to sell U.S. Savings Bonds directly to the public. According to Treasury, the system generated almost $230 million in bond sales in its first 18 months of operation.

- *Government-to-Employee.* Electronic government can be used to more effectively interact with employees to enhance productivity and human resources management. The Office of Personnel Management's *Employee Express* is an automated system enabling federal employees to initiate the processing of certain discretionary personnel and payroll transactions. For example, using *Employee Express*, employees can change data related to their Thrift Savings Plan accounts and health benefits, thus offering an alternative to paper forms. An example of an agency-specific initiative is *lifelines*, the Navy's Web-based quality of life (QOL) program and services delivery system. Inaugurated in January 1999 (and redesigned in June 2000), *lifelines* is built on five core business areas, the (1) "QOL Network," which includes access to quality of life information and services, (2) "QOL News Center," which provides access to the news, (3) "QOL Broadcast Network," which brings stories and video clips to sailors, Marines, their families, and others using video streaming and electronic publishing technology, (4) "QOL Business Innovations Portal," which includes Department of Defense and Department of the Navy on-line administrative and service delivery processes, and (5) "QOL Gateway," which has thousands of links to service providers.

[13] *http://www.seniors.gov.*

- *Government-to-Government.* One goal of digital government is to provide access and interaction with government services on a functional or topical basis, rather than being focused on the specific agency or agencies responsible for administering programs and policies. For example, our February report on technology-based regulatory innovations noted examples of such innovations that involved interagency or intergovernmental cooperation.[14] In one case, the interagency Integrated Government-wide International Trade Data System is designed to enable various federal trade agencies to share a standard set of data to enable the more efficient electronic release of goods, conveyances, and crews. According to the developers, the system is expected to provide the primary inspector with "one look" at the truck, its goods, and the driver's compliance with key federal requirements before the truck enters the United States. In another example, the Environmental Protection Agency is working on an intergovernmental e-government initiative—*the National Environmental Information Exchange Network*—that the agency believes can improve both the quality of and access to environmental data. The exchange network is to be a voluntary, standards-based system that links different state systems and the Environmental Protection Agency's systems, using common language and secure connections through the Internet. In October 2000, a team comprising participants from the Environmental Protection Agency, individual states, and the Environmental Council of the States released a blueprint that lays out the network design and partnership agreements for implementing the network.

- *Government-to-Business.* E-government projects have also been initiated to more effectively work with businesses as suppliers of goods and services and as regulated economic sectors. For example, the General Services Administration's *FedBizOpps* has been designated as the single governmentwide point of electronic entry for access to federal government business opportunities greater than $25,000.[15] Using this Web site, sellers and service providers can access and download information such as solicitations. Moreover, after subscribing, vendors can receive various announcements

[14] *Regulatory Management: Communication About Technology-Based Innovations Can Be Improved* (GAO-01-232, February 12, 2001).

[15] This designation was published as an interim Federal Acquisition Regulation on May 16 (it is open for public comment until July 16, 2001). The interim rule gives federal agencies until October 1, 2001, to complete their transition to, or integration with, *FedBizOpps*. After October 1, all agencies must use *FedBizOpps* to provide the public access to notice of procurement actions over $25,000.

automatically via e-mail, including presolicitation and post-award notices and their amendments and notices of solicitation and solicitation amendment releases. According to the General Services Administration, as of mid-May, over 90,000 vendors were registered to receive notification of business opportunities from *FedBizOpps.* Another example of a government-to-business initiative is the Department of Labor's Employment Laws Assistance for Workers and Small Businesses, or *elaws* application.[16] *Elaws* provides interactive advice through the Internet to help small businesses and workers understand their rights and responsibilities under federal employment laws and regulations. Each *elaws* "advisor" imitates the interaction that an employer or employee might have with a Department of Labor employment law expert, asking questions and providing answers based on the responses provided.

Many Internet-based initiatives can be relatively easy to implement and have a potentially high payoff for increasing the speed and efficiency with which citizens and businesses interact with the government. For example, the immediate placement of high-demand documents or information on an agency's Web site can help improve citizens' satisfaction with government responsiveness as well as result in potential cost savings by reducing the need for distributing printed copies. One example of such an initiative is *FedForms.gov*, which provides "one stop shopping" for the forms needed for the top 500 government services used by the public. Other potentially high-payoff initiatives, however, may be more difficult and time-consuming to fully implement. For example, allowing citizens to more easily access their personal information maintained by government agencies, which can be beneficial to the individual, must address difficult privacy and security issues. Indeed, the Social Security Administration has been cautious in pursuing its on-line initiatives largely in view of the privacy and security concerns raised following its implementation of the on-line personal earnings and benefits estimate statement.[17] As I will discuss in a moment, risks involving issues such as privacy can be addressed and managed, with the implementation of appropriate management and technical policies and controls.

[16] GAO-01-232, February 12, 2001.

[17] The Social Security Administration's on-line personal earnings and benefits estimate statement 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).

Significant Challenges in Transitioning to E-government

The many federal initiatives demonstrate the opportunities for the growing use of e-government to provide faster, more convenient, and more efficient on-line information access and services to citizens. However, past mistakes serve to remind us that technology solutions often involve varying levels of risks in addition to expected benefits. Let me address some of the areas needing attention as e-government moves forward. None are insurmountable, but they deserve attention and must be addressed to ensure successful e-government outcomes.

Sustaining Committed Executive Leadership

As in the case with well-run commercial entities, strong leadership and sound management are central to the effective implementation of public-sector policies or programs. Moreover, our wide-ranging work on federal management issues has shown that perhaps the single most important element of successful management improvement initiatives is the demonstrated commitment of top leaders to change.[18] Top leadership involvement and clear lines of accountability for making management improvements are critical to overcoming organizations' natural resistance to change, marshalling the resources needed in many cases to improve management, and building and maintaining the organizationwide commitment to new ways to doing business.

In our studies of leading private and public-sector organizations in IT management, we have also noted that effective top management leadership, involvement, and ownership are a cornerstone of any information technology strategy.[19] For example, we have previously reported that strong and focused leadership was a pivotal factor leading to the government's successfully meeting the Year 2000 computing challenge and that this lesson should be applied to other ongoing major management challenges.[20] We concluded that as the federal government moves to fully embrace the digital age and focuses on e-government initiatives, comprehensive and focused leadership is of paramount importance. We

[18] *Management Reform: Elements of Successful Improvement Initiatives* (GAO/T-GGD-00-26, October 15, 1999).

[19] *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology* (GAO/AIMD-94-115, May 1994) and *Executive Guide: Maximizing the Success of Chief Information Officers, Learning From Leading Organizations* (GAO-01-376G, February 2001).

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

have also emphasized the importance of strong senior leadership support in areas such as IT investment, performance measurement, and security.[21]

Earlier this year we reported on the need for agency leadership in the IT arena at the Departments of Veterans Affairs and Agriculture. In April we testified that successful implementation of the Department of Veterans Affairs' IT program requires strong leadership and management among a CIO and other senior executives to help define and guide the department's plans and actions.[22] To his credit, the newly appointed Secretary of Veterans Affairs had identified filling the department's CIO position as one of his top priorities, and at the time of the hearing, was conducting an extensive search to identify suitable candidates for the position, which requires Senate confirmation. At the April hearing, the Secretary of Veterans Affairs also stated that he was providing his "personal commitment that we will reform the way we use information technology" at the department and he emphasized his commitment to the development of an enterprise architecture and security issues.[23] At the Department of Agriculture, we reported[24] in February that the department had not assigned a senior-level official with overall responsibility and accountability for managing and implementing separate activities related to the Freedom to E-File Act (P.L. 106-222).[25] As a result of this and other concerns, we reported that, while Agriculture had made progress and had partially met the E-File Act's initial deadlines, it faced formidable challenges in meeting future deadlines.

Building an E-government Business Case

Agencies have reported expending over $41 billion in IT investments in fiscal year 2000 and have proposed to increase this to nearly $45 billion in fiscal year 2002.[26] A primary challenge for agencies in moving toward e-

[21] *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (AIMD-10.1.23, Exposure Draft, May 2000), *Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments* (GAO/AIMD-98-89. March 1998) and *Executive Guide: Information Security Management* (GAO/AIMD-98-68, May 1998).

[22] *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist* (GAO-01-550T, April 4, 2001).

[23] Testimony of Anthony J. Principi, Secretary, Department of Veterans Affairs before the House Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, April 4, 2001.

[24] *USDA Electronic Filing: Progress Made, But Central Leadership and Comprehensive Implementation Plan Needed* (GAO-01-324, February 28, 2001).

[25] The Freedom to E-File Act (P.L. 106-222) requires the Department of Agriculture to establish an electronic filing and retrieval system to enable farmers and other agricultural producers to access and file paperwork electronically

[26] *Report on Information Technology (IT) Spending for the Federal Government for Fiscal Years 2000, 2001, and 2002* (OMB).

government is to implement and follow management practices that help ensure IT dollars are directed toward prudent investments that focus on achieving cost savings, increasing productivity, and improving the timeliness and quality of service delivery. Even with its legislatively mandated deadline, according to OMB's GPEA guidance, the act recognizes that building and deploying electronic systems to complement and replace paper-based systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission, protect privacy, and ensure the security of the data.

Accordingly, like any other information technology project, electronic government initiatives should be supported by a well-developed business case that evaluates the expected returns against the costs. An explicit understanding of the costs and expected benefits up front provides the basis for a sound financial and strategic decision and creates a baseline for managers and executives to measure progress against. Moreover, improvements in quality, cost-effectiveness, speed of service delivery, or operational effectiveness should provide key information for investment decisionmakers. The business case provides the forum for the evaluation of the projects' costs, benefits, and integration with the agency performance and results strategy. In addition, the business case provides assurance to agency executives that key factors of the proposed system have been adequately thought out and planned for.

In government's rush to provide greater electronic service delivery, it is essential for agency executives to remember that fundamental principles and practices of good IT planning and management apply equally to effective customer-centric Web-based applications. As we noted in May 2000,[27] some of these fundamentals include

- developing a well-defined project purpose and scope and realistic, measurable expectations;
- understanding and improving business processes before applying technology;
- performing risk assessments and developing appropriate risk mitigation strategies;
- using industry standard technology and solutions where appropriate;

[27] GAO/T-AIMD/GGD-00-179, May 22, 2000.

- adopting and abiding by pertinent data standards;
- thoroughly training and supporting users; and
- reviewing and evaluating performance metrics.

Maintaining a Citizen Focus

Today, governments at all levels increasingly recognize the individual citizen and citizen “communities of interest” as customers. However, translating this growing awareness into better, efficient, and friendly services can be challenging. Just as the Internet and Web-based technologies should force organizations to rethink their business processes, they should also force organizations to reconsider their customers—specifically how their customers need, perceive, and digest information and services in a viewable, electronic format. For example, private industry Web sites are increasingly being tailored to allow for individual preferences and needs to restrict information only to those products and services desired. “Interactive” consumers meanwhile are starting to demand even more convenience and operational excellence from the on-line companies they deal with on a regular basis. These practices, however, pose privacy questions for the federal government, which I will discuss in the next section.

One initiative that seems to be an example of a citizen focus is the *Government Without Boundaries* project. Launched at a September 2000 meeting of federal, state, and local CIOs, this project recognizes that citizens and businesses may not differentiate among levels of government when seeking government services. As a result, the General Services Administration along with other federal agencies such as the Department of the Interior, are working with selected state and local governments with the goal to create a virtual pool of on-line government information and services from all levels. For example, the Virginia project under *Government Without Boundaries*, which is being conducted in association with Fairfax County and the city of Virginia Beach, is a model Web-enabled registry of youth services across all levels of government. The New Jersey project, being conducted with Monmouth County, is a pilot demonstration of a shared calendar of park events that contains information on local, state, and federal parks.

Maintaining a citizen focus does not stop with the implementation of Web sites. Another key component is developing customer support tools to assist the public’s use of such mechanisms. For example, the National Electronic Commerce Coordinating Council suggests that organizations implement a customer relations management structure that could include (1) a telephone support service to respond to user questions, (2) an on-line support function accessible directly from the Web site, (3) tools to monitor and track problems and user questions, and (4) processes to analyze user traffic.[28]

Protecting Personal Privacy

On-line privacy has emerged as one of the key—and most contentious—issues surrounding the continued evolution of the Internet. In particular, the federal government faces challenges in ensuring personal privacy while also continuing to implement and expand e-government. A national survey found that Americans believe that e-government has the potential to improve the way that government operates but a majority also had concerns about sharing personal information with the government over the Internet, fearing that the data will be misused and their privacy diminished.[29]

Federal agencies are required by law to protect an individual's right to privacy when they collect personal information. The Privacy Act of 1974, as amended, is the primary law regulating the federal government's collection and maintenance of personal information, and requires protection of personal information maintained in an agency's system of records.[30] Since the passage of the act, however, advances in information technology and the increasing use of the Internet have raised concerns about the adequacy of the act's provisions. In response to such concerns, Mr. Chairman, you and the Chairman of the House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations have asked us to conduct a comprehensive review of agency compliance with the Privacy Act and identify privacy issues that are not adequately covered by the act. This work is ongoing, and we expect to issue our first report early next year.

In addition to the Privacy Act, OMB has issued guidance specifically focused on Internet privacy. For example, in June 1999 it issued a memorandum directing executive departments and agencies to post clearly labeled and easily accessed privacy policies on their principal Web

[28] *E-Government Strategic Planning: A White Paper* (National Electronic Commerce Coordinating Council, December 13, 2000).

[29] August 2000 Hart-Teeter survey reported in *e-government: The Next American Revolution*, The Council for Excellence in Government, February 2001.

[30] P.L. 93-579, 5 U.S.C., section 552a.

sites. In September 2000, we reported[31] that most—67 of 70—principal Web sites we reviewed had posted privacy policies that were clearly labeled and easily accessed—a considerable improvement over a 1999 survey of selected federal sites by a public interest group.[32] However, we also found that of 31 high-impact agencies,[33] most did not post a privacy policy on all Web pages that collected personal information as required by OMB. In addition, of 101 on-line forms that we reviewed, 44 did not have a privacy policy posted on the Web page. We recommended that OMB, in consultation with the CIO Council and others, consider clarifying certain aspects of its guidance and determine whether existing oversight strategies were adequate to ensure agency adherence to the web site privacy policies.

OMB has also issued specific guidance concerning federal agency use of Internet "cookies." Cookies are text files that have unique identifiers associated with them, and are used to store and retrieve information that allows Web sites to recognize returning users, track on-line transactions, or maintain and serve customized Web pages. "Session" cookies expire when the user exits the browser, while "persistent" cookies remain on the user's computer for a specified length of time, which may be years. Although cookies can be used to enable electronic commerce and other applications, persistent cookies also pose privacy risks even if they do not gather personally identifiable information because the data contained in them can be subsequently linked to the individual. Because of such concerns, OMB issued guidance in June 2000 directing that cookies not be used on federal Web sites unless certain conditions were met, including a compelling need and approval by the head of the agency. In September 2000, in response to inquiries about the scope of the guidance, OMB further clarified its policy in a letter to the CIO Council stating that it applied only to persistent cookies.

Our work conducted within the past year on the use of cookies illustrates the challenges that OMB and federal agencies face in balancing increased use of the Internet to provide information and deliver services against

[31] *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy* (GAO/GGD-00-191, September 5, 2000).

[32] An April 1999 report by the Center for Democracy and Technology *(Policy vs. Practice: A Progress Report on Federal Government Privacy Notices on the World Wide Web*) stated that just over one-third of 46 federal agencies had privacy policies linked from their home pages, 8 agencies had privacy policies that were not on their home pages, and 22 agencies did not have privacy policies.

[33] The National Partnership for Reinventing Government identified 31 agencies as having high impact—that is they have 90 percent of the federal government's contact with the public.

concerns over privacy.[34] As we reported in April 2001, OMB's guidance on the use of cookies, while helpful, left agencies to implement fragmented directives contained in multiple documents. Further, the guidance itself was not clear on the disclosure requirements for techniques such as session cookies. We concluded that OMB's stated position that agencies were not required to disclose the use of session cookies could lead to confusion on the part of visitors to federal Web sites. As a result of these concerns, we recommended that OMB, in consultation with other parties, (1) unify its guidance on Web site privacy policies and the use of cookies, (2) clarify the resulting guidance to provide comprehensive direction on the use of cookies by federal agencies on their Web sites, and (3) consider directing federal agencies to disclose in the use of session cookies in their Web site privacy notices.

Implementing OMB's cookie guidance requires constant agency diligence and attention. In our April report we noted that, as of January 2001, most of the federal Web sites that we reviewed were following OMB's guidance on the use of cookies. However, of the 65 sites we reviewed, eight sites using persistent cookies did not comply with OMB's requirements for such use. These agencies all took or planned to take corrective action. Further, last month, the DOD Inspector General issued a report summarizing the results of 51 Inspector General reports from other agencies, which identified the use of 300 persistent cookies at 22 agencies' Web sites. In the vast majority of cases, these persistent cookies were not approved by the agency head, as required by OMB.

Privacy issues extend beyond what is disclosed on and the data captured by Web sites, and can involve complicated and controversial issues. An example is the implementation of the Department of Health and Human Services' (HHS) privacy regulations mandated by the Health Insurance Portability and Accountability Act of 1996.[35] As we testified this past February, this regulation represents an important advancement in the protection of individuals' health information.[36] At the same time, however, we noted that health care providers faced a complex new set of privacy requirements that were not well understood. In February, the Secretary of HHS requested public comments on this regulation, stating that this was

[34] *Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies"* (GAO-01-424, April 27, 2001) and *Internet Privacy: Federal Agency Use of Cookies* (GAO-01-147R, October 20, 2000).

[35] P.L. 104-191, 264, 110 Stat. 1936, 2033.

[36] *Health Privacy: Regulation Enhances Protection of Patient Records but Raises Practical Concerns* (GAO-01-387T, February 8, 2001).

needed to help the department assess its “real-world” impact in health care delivery. During the 30-day comment period, HHS reported that it received more than 11,000 letters or comments. Just last week HHS issued the first of what is expected to be several technical assistance materials to clarify and help covered entities implement the regulation. In this guidance, HHS provided examples of some of the changes to the regulation that it expects to propose. For example, HHS stated that it would propose a change that would permit pharmacists to fill prescriptions phoned in by a patient’s doctor before obtaining the patient’s written consent.

Implementing Appropriate Security Controls

Security concerns present one of the toughest challenges to extending the reach of electronic government. Even if federal agencies adopt policies and procedures designed to protect the privacy of sensitive electronic information, that information could still be compromised if the security of the Web servers, operating systems, and software applications involved is inadequate. The rash of hacker attacks, Web page defacing, and credit card information being posted on electronic bulletin boards can make many federal agency officials—as well as the general public—reluctant to conduct sensitive government transactions involving personal or financial data over the Internet.

These concerns are not unjustified. We have designated information security as a governmentwide high risk area since 1997. Our latest high-risk report noted that progress in strengthening federal information security has been mixed.[37] Efforts to address the problem had gained momentum but audits showed that federal operations and assets continued to be highly vulnerable to computer-based attacks.

In recent years we have consistently found security weaknesses at many federal agencies, ranging from security program management to access controls to segregation of duties.[38] For instance security weaknesses at agencies such as IRS, the Centers for Medicare and Medicaid Services (formerly known as the Health Care Financing Administration), the Social Security Administration, and the Department of Veterans Affairs could place sensitive tax, medical, and other personal records at risk of unauthorized disclosure. As we recently reported, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing

[37] *High-Risk Series: An Update* (GAO-01-263, January 2001).

[38] For example, see *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk* (GAO-01-600T, April 5, 2001) and *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

systems or to the electronically transmitted tax return data those systems contained.[39] Unauthorized individuals could have gained access to IRS' electronic filing systems and modified taxpayer data contained in those systems during the 2000 tax-filing season. IRS reports that it has substantially corrected the access control weaknesses cited in that report. Nevertheless, failure to maintain adequate security over IRS' electronic systems in the future could erode public confidence in filing tax returns electronically.

A key element in promoting the expansion of electronic government is providing citizens with the capability to conduct the full range of their government business—including sensitive transactions such as benefit applications—on-line. Effective information security is essential to the increased implementation of electronic transactions. For example, unless special security features are properly implemented, electronic transactions can be more susceptible to fraud and abuse than traditional paper-based transactions. While a paper record of a transaction can undergo forensic chemical analysis to determine whether it has been altered, knowledgeable individuals can alter electronic records in systems virtually without detection. Further, physical access must occur before a paper record can undergo tampering but with the enhanced global systems interconnectivity made possible by the Internet, physical access is not necessary. Instead, electronic misuse and tampering can occur more quickly and with far greater impact if inadequate safeguards are not in place. Finally, human participation is required on both sides of a paper-based transaction, providing the opportunity for immediate human inspection and verification of the transaction. In contrast, electronic systems may readily process transactions that would be immediately suspicious to a human observer.

An important piece of the solution to the Internet-based security problem will be the development and implementation of so-called Public Key Infrastructure or PKI technology (a system of computers, software and data that relies on certain sophisticated cryptographic techniques to secure on-line messages or transactions). According to the Principal Deputy CIO of the Department of Defense, "the path to electronic transactions is closely coupled to the maturation and affordability of the PKI."[40] A properly implemented and maintained PKI can offer important

[39] *Information Security: IRS Electronic Filing Systems* (GAO-01-306, February 16, 2001).

[40] Joint Statement of John L. Osterholz, Principal Deputy Chief Information Officer, Department of Defense, and Norma J. St. Claire, Director, Information Management for Personnel and Readiness, Office of the Secretary of Defense, before the House Committee on Government Reform, June 21, 2001.

security services, including assurance that (1) the parties to an electronic transaction are really the people they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny that they took part in the transaction.

As we reported in February, progress has been made in seeding PKI technology throughout the government.[41] However, a number of substantial challenges must be overcome before the technology can be widely and effectively deployed. For example, it is not yet fully known whether this technology will be truly scalable[42] and interoperable[43] as its use grows. Further, the costs of building a PKI and enabling software applications to use it can easily add up to millions of dollars. Moreover, there is a range of policy and human capital issues to consider. In addition, because federal agencies are adopting different and incompatible implementations of PKI technology, the development of the Federal Bridge Certification Authority is critical. The federal bridge is being designed to link disparate agency PKI systems and promote PKI interoperability within and outside the federal government. Without a successfully functioning bridge, agencies will need to individually make arrangements to interoperate with other specific agencies in order to share secure information or transactions. Such a process would likely be tedious and impractical.

Maintaining Electronic Records

In implementing GPEA and moving toward e-government, executive-branch agencies and the National Archives and Records Administration (NARA) will be faced with the substantial challenge of preserving electronic records in an era of rapidly changing technology. Agencies must create electronic records, store them, properly dispose of them when appropriate, and send permanently valuable records to NARA for archival storage. For e-mail alone, this involves the huge volumes of e-mail agency employees now send and receive in performing their official duties. Moreover, staff members creating records need to be made aware of what constitutes an electronic record, how to save it, and how to archive it for future use.

[41] *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology* (GAO-01-277, February 26, 2001).

[42] Scalability is the ability to easily change in size or configuration to suit changing conditions.

[43] Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

When deciding how to store electronic documents, agencies must take into account the legal viability of the records they create. The Department of Justice's guidance for federal agencies on designing and implementing electronic processes notes that the adoption of electronic systems or the conversion of paper-based records systems to electronic ones can present significant legal issues that need to be identified and addressed as part of the decision-making process.[44] As with paper-based records, electronic records need to be available, reliable, and pursuasive. According to Justice, some of the issues related to electronic records retention that need to be addressed include (1) providing the continued capability to access information from older technology, (2) having staff who are familiar and competent to work with the electronic processes necessary to read older data, and (3) ensuring that steps are taken to preserve passwords or other data to be able to retrieve information that was encrypted or otherwise protected.

The long-term preservation and retention of those electronic records is a challenge for agencies and NARA. For example, NARA, in its guidance, remarked that hardware and software obsolescence can make record-retention burdensome. Moreover, the NARA guidance developed in response to GPEA recognizes that records management involving records that have been created using electronic signature technology is a complex process, requiring training and knowledge on the part of both IT specialists and records management personnel. Further, NARA itself must be able to receive electronic records from agencies, store them, and retrieve them when needed. To do so, it must expand its capacity to accept an increasing volume of electronic records from agencies. In addition to the increasing volume, the variety of electronic records such as word processing documents, e-mail messages, databases, digital images, and Web site pages complicates NARA's mission to preserve these records. In response to this challenge, in July 1999 NARA initiated the Electronic Records Archives program. Under this program NARA intends to develop a system that would assemble, manage, preserve, and make available vast amounts of diverse electronic government records.

Maintaining a Robust Technical Infrastructure

An important key to success in e-government is to plan for and implement an adequate technical infrastructure that will support a user's experience of easy and reliable electronic access across government. Among the elements of a supporting technical infrastructure that are important to

[44] *Legal Considerations in Designing and Implementing Electronic Processes: A Guide For Federal Agencies* (Department of Justice, November 2000).

ensuring the successful implementation of e-government initiatives are the following:

- *Adequate network capacity, or bandwidth.* Government agencies need to consider the amount of electronic traffic that will be generated by an electronic offering and provide adequate resources to support that load. As we reported in September 2000, some Web sites have been completely overwhelmed and disabled when far greater numbers of users visited the sites than their developers anticipated.[45]

- *System and platform reliability.* The Web servers and other computer platforms that support e-government services—including their operating systems and the software that connects them—must also be capable of supporting potentially heavy user demands and must run reliably. The systems must reliably (1) confirm that a transaction is complete and (2) abort a transaction completely and consistently in the event that some problem arises. In the private sector, customers generally expect e-businesses to be up and running 24 hours a day, 7 days a week, providing smooth, efficient transactions without significant delays. Electronic government will likely need to meet this standard. Providing such continuous, reliable service for potentially large numbers of customers requires careful planning and design. Where heavy traffic is expected, for example, load balancers may be needed to intercept Web traffic going to an agency's site and efficiently distribute it among an array of servers to prevent any one system from becoming overwhelmed and to provide automatic immediate backup in the event that a particular machine fails.

- *Technology Alternatives.* As we noted in May 2000, the government's Web-based applications are not necessarily the only incarnation that e-government will take.[46] As more of the public moves to compact wireless devices, the government will need to ensure that its applications are accessible by more than just a small number of end-user systems, or platforms. In all likelihood, a variety of media will be needed for conducting transactions, from traditional paper-based methods on one end of the spectrum to small wireless receivers on the other.

[45] GAO/AIMD-00-282, September 15, 2000.

[46] GAO/T-AIMD/GGD-00-179, May 22, 2000.

- *Technology refreshment.* As technology continues to evolve, government will be challenged to enhance existing electronic applications to incorporate new technologies and provide better service. A good example is the federal government's *FirstGov* Web portal. Last year we noted that the inauguration of *FirstGov* represented a significant achievement in that an important and previously unavailable capability—searching the entire government's Web pages—was rapidly and successfully put into place.[47] Without detracting from that accomplishment, we also noted that *FirstGov's* search engine was not particularly context-sensitive. In other words, if a given search did not produce helpful information, it was up to the user to define and redefine the search in ways that might return more meaningful information. *FirstGov* officials are taking steps to improve their search technology, such as adding links to the states and defining and incorporating key words that will trigger predefined results. These and other enhancements will be needed as search technology advances. If *FirstGov* is not continually enhanced to provide better results to citizens' queries, the initial luster of the government's accomplishment may soon fade.

In addition, even a smoothly operating electronic delivery service will fail to fulfill the promise of e-government if it is isolated from or unable to work with other related applications. Many e-government applications clearly need to communicate among themselves and exchange relevant data—especially those involved in processing transactions. The Extensible Markup Language, or XML, is one recent technology development that may help in this regard, although its ultimate role is not yet known. Mr. Chairman, at your request, we are conducting a study on the use of XML in the federal government. Our work is not yet complete, however, at your request we are providing some information on this topic.

XML provides a standard way to tag or "mark up" pieces of information so that they can be readily identified and exchanged among disparate computer applications. XML holds the promise of facilitating transactions and bringing together data from computer systems that previously were difficult to access and integrate. For example, a pilot project is underway to enhance the successful *FedStats.gov* Web site through the use of an XML-based "content network." Instead of simply being a repository for statistical data that is updated only at certain specified times, the XML-based *FedStats* site would link users directly to the source data within

[47] *Electronic Government: Opportunities and Challenges Facing the FirstGov Web Gateway* (GAO-01-87T, October 2, 2000).

individual agencies, significantly enhancing their ability to access needed data.

Some formidable organizational challenges must be met before the potential of XML can be fully realized. XML, by design, stops short of defining specific data standards, such as the data fields that might appear on an electronic application form or the protocols necessary to conduct complete business transactions. Therefore, consensus must be reached—both in the private sector as well as in government—on how to set such standards and conform to them in a meaningful way. Moreover, a number of industry organizations are already using XML to define their own vocabularies for business relationships and transactions. Examples include electronic business XML (ebXML)—a set of specifications that together act as a complete, modular framework so that anyone can do business with anyone else over the Internet—and the Extensible Business Reporting Language (XBRL), a specification for reporting financial information that enhances the transfer and analysis of that information. The federal government will need to determine which of the many developing XML standards it intends to adopt, and agencies will need incentives to comply with the specific XML data formats that emerge as governmentwide standards.

A first step in this direction would be the establishment of a governmentwide registry, where specific XML data standards could be collected and referenced. Such a registry would allow early XML adopters to share information on the data formats they are using and could assist in determining what standards to adopt in the future. The CIO Council's XML Working Group has sponsored an effort with the National Institute of Standards and Technology and the General Services Administration to develop a pilot for such a registry, although work still needs to be done to define how the registry should be administered and maintained on an ongoing basis. The establishment of this registry will be critical to the success of XML as a broad facilitator of information exchange.

Human Capital: IT Workforce Management

The demand for IT workers is high and growing. The Bureau of Labor Statistics projects that the demand for computer systems analysts, engineers, and scientists will almost double between 1998 and 2008 and the demand for computer programmers will increase by 30 percent during the same time period.[48] In September 2000, we reported that to enhance

[48] "*The 1998-2008 job outlook in brief" (Occupational Outlook Quarterly, Bureau of Labor Statistics, Spring 2000).*

U.S. workers' ability to fill IT positions, the Department of Labor and the National Science Foundation were working to improve the IT skills of the U.S. workforce.[49] The employers we contacted told us that they are also trying to improve U.S. workers' IT skills, and identified a variety of short-term methods, such as retraining new or existing employees, to provide U.S. workers with the needed skills.

The need for qualified IT professionals puts governments in direct competition with the private sector for scarce resources. In addition, the increasing government reliance on private sector service providers and outsourced application development has created a growing demand in the federal workplace for more traditional skills, such as sourcing and contract management and project and program management.

With respect to the federal government, another major concern is that a substantial portion of the federal workforce will retire between fiscal years 1999 and 2006. We recently estimated that by 2006 about 31 percent[50] of 24 major departments and agencies' employees working in 1998 will be eligible to retire, and that through the end of 2006 about half of those eligible will actually retire.[51] In addition, all 24 major departments and agencies reported that the computer specialist series was considered mission-critical occupations and we estimated that 30 percent of employees in this series would be eligible to retire by the end of fiscal year 2006, and that 14 percent would retire by then.

To help address IT human capital issues, the CIO Council and the Administrative Office of the U.S. Courts asked the National Academy of Public Administration (NAPA) to study IT compensation strategies and to make recommendations on how the government can best compete for IT talent. NAPA has completed and reported on the first phase of this study. Table 1 summarizes NAPA's overall comparison of compensation and work factors among various sectors, which demonstrates some of the similarities and differences among the sectors. NAPA's high, medium, and low designations shown below are based on an overall evaluation of data

[49] *H-1B Foreign Workers: Better Controls Needed to Help Employers and Protect Workers* (GAO/HEHS-00-157, September 7, 2000).

[50] The eligibility estimate of 31 percent is based on cumulative data, which includes those already eligible and those reaching retirement eligibility between fiscal years 1999 through 2006, less the estimated 4 percent who are estimated to leave before they become eligible to retire.

[51] *Federal Employee Retirements: Expected Increase Over the Next 5 Years Illustrates Need for Workforce Planning* (GAO-01-509, April 27, 2001).

and information obtained for organizations in each sector in comparison with the other sectors.

Table 1: Overall Comparison of Compensation and Work Factors

Sector	Salary levels	Work-life benefits	Rewards/ recognition	Advancement/ training	Use of recruiting tools
Federal	Low	High	Low	Low	Low
State	Low	Medium	Medium	Medium	Medium
Local	Low	Medium	Medium	Low	Low
Nonprofit	Medium	Medium	Medium	Medium	High
Private	High	High	High	High	High
Academia	Medium	High	Medium	Medium	Medium

Source: *Comparative Study of Information Technology Pay Systems: Executive Study* (NAPA, March 2001).

NAPA's final report is expected to be completed by mid-September and will contain an evaluation of alternative compensation models and address recommended solutions.

Without fully developing staff capabilities, agencies stand to miss out on the potential customer service benefits presented by technology. Employees must have the training and tools they need to do their jobs. The process of adopting a new system can be made much less difficult by offering well-designed, user-oriented training sessions that demonstrate not only how the system works, but how it fits into the larger work picture and "citizen as customer" orientation. A significant challenge for all agencies is providing internal incentives for customer service, reducing employee complaints, and cutting the time employees spend on non customer-related activities.

Ensuring Uniform Service to the Public

An important policy consideration governments face is how to provide services and access to those segments of the population with limited Internet access and ensure their participation in this new electronic environment. While an October 2000 Department of Commerce report[52] found that the overall level of U.S. digital inclusion is rapidly increasing,

[52] *Falling Through The Net: Toward Digital Inclusion* (U.S. Department of Commerce, October 2000).

with gains being made by groups that have traditionally been digital "have nots," a digital divide remains or has expanded slightly in some cases. For example, (1) people with a disability are only half as likely to have access to the Internet as those without one, (2) large gaps for Blacks and Hispanics remain when measured against the national average, and (3) individuals 50 years of age or older are among the least likely to be Internet users.

The challenge for policymakers in the long run will be to determine whether any *continuing* disparities in the availability and use of the Internet among different groups of Americans threaten to offer citizens separate levels of service and access. This presents an immediate and complex leadership challenge confronting government policymakers and managers: 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. Multiple access methods to government services and processes—in person, by phone, via fax, using public kiosks—may be essential to supplement Internet use.

The Congress has taken action to address the digital divide that confronts people with disabilities. Specifically, the Workforce Investment Act of 1998[53] (section 508 of the Rehabilitation Act, 29 U.S.C. 794d) requires federal departments and agencies and the U.S. Postal Service to procure, develop, maintain, and use electronic and information technology[54] that is accessible for people with disabilities—including both federal employees and members of the public—unless an undue burden would be imposed on the department or agency. An April 2000 Department of Justice report[55] to the President on this law, which was based on section 508 self-evaluations conducted by federal agencies in 1999, indicated that while several agencies are models for accessibility, others need improvement. Justice also reported that (1) federal agency Internet and Intranet sites contained some barriers to access for people with disabilities, (2) almost all software applications contained some barriers to some people with disabilities, although most provided a fair degree of accessibility to most people with

[53] P.L. 105-220

[54] Electronic and information technology is defined as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

[55] *Information Technology and People with Disabilities: The Current State of Federal Accessibility* (Department of Justice, April 2000).

disabilities, and (3) telecommunications posed specific accessibility issues for almost every community of persons with disabilities and few agencies were fully utilizing available services such as the Federal Information Relay Service (which allows deaf and hard of hearing people to communicate via telephone with people who do not have special equipment). The Department of Justice is due to submit another report to the President on this issue by August 7 of this year. This report is expected to focus on the accessibility of federal agencies' Web sites.

As called for by this law, on December 21, 2000, the Architectural and Transportation Barriers Compliance Board[56] published its final rule, which became effective on June 21, on electronic and information technology accessibility standards. A little over 4 months after these standards were published, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council published a final rule amending the Federal Acquisition Regulation to incorporate these standards, which became effective June 25.

Recently, the National Council on Disability[57] reported that individual leadership and commitment on the part of officials and staff, particularly at federal agencies, largely accounted for the relative success in implementing pro-accessibility measures.[58] However, the council cautioned that the institutionalization of these practices and policies remains tenuous. Accordingly, the council made a series of recommendations for implementing and enhancing current laws and practices. For example, the council recommended that (1) OMB provide guidance on documenting the integration of accessibility considerations into agency information technology polices, practices, and decisions, (2) individual agencies and the Department of Justice develop a system for random periodic auditing of Web sites to ensure that standards of accessibility are maintained, and (3) the Department of Justice develop a procedure for verifying agency self-reporting of progress.

[56] The Architectural and Transportation Barriers Compliance Board is an independent agency whose primary mission is to promote accessibility for individuals with disabilities. The board consists of 25 members, 13 of whom are appointed by the President, a majority of who are required to be individuals with disabilities. The other 12 members are from various federal agencies, such as the Departments of Defense, Health and Human Services, and Veterans Affairs, and the U.S. Postal Service.

[57] The National Council on Disability is an independent federal agency with 15 members appointed by the President and confirmed by the Senate. The Council promotes policies, programs, practices, and procedures that guarantee equal opportunity for all individuals with disabilities and to empower individuals with disabilities to achieve economic self-sufficiency, independent living, and inclusion and integration into all aspects of society.

[58] *The Accessible Future* (National Council on Disability, June 21, 2001).

Proposed Legislation Would Establish a Federal CIO Who Could Address E-government Challenges

The many challenges associated with the effective implementation of e-government initiatives require strong central leadership to overcome. Mr. Chairman, in introducing S. 803, the *E-Government Act of 2001,* you have recognized this need and have sought to provide it through the establishment of a federal CIO.

As we have previously testified, the government's current information resources and technology management framework can be strengthened by establishing a central focal point, such as a federal CIO.[59] Clearly, departments and agencies should have the primary responsibility and accountability for decisions related to IT investments and spending supporting their missions and statutory responsibilities. But governmentwide issues need a strong catalyst to provide substantive leadership, full-time attention, consistent direction, and priority-setting for a growing agenda of government issues, such as e-government, security, and large-scale IT investments. A federal CIO could serve as this catalyst, working in conjunction with other executive officials to ensure that information resources and technology management issues are addressed within the context of the government's highest priorities and not in isolation from them.

During the period of the legislative deliberations on the Clinger-Cohen Act, we supported strengthened governmentwide management through the creation of a formal CIO position for the federal government.[60] More recently, in September 2000 we called for the Congress to consider establishing a formal CIO position for the federal government to provide central leadership and support.[61] As we noted then and reemphasized in April,[62] a federal CIO would 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 overseeing federal agency information technology and management

[59] *Federal Chief Information Officer: Leadership Needed to Confront Serious Challenges and Emerging Issues* (GAO/T-AIMD-00-316, September 12, 2000).

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

[61] GAO/AIMD-00-290, September 12, 2000.

[62] *Information and Technology Management: Achieving Sustained and Focused Governmentwide Leadership* (GAO-01-583T, April 3, 2001).

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. A federal CIO could also participate in establishing funding priorities, especially for crosscutting e-government initiatives such as the President's proposed e-government fund (estimated to include $100 million over 3 years), which is expected to support interagency e-government initiatives.

Consensus has not been reached within the federal community on the need for a federal CIO. Even individuals or organizations that support a federal CIO disagree on the structure and authorities of such an office. In addition, while CIOs or equivalent positions exist at the state level 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. Our research has also found that diversities in corporate missions, structures, cultures, and capabilities prohibit a prescriptive approach to information management leadership.[63] Instead, executives in leading organizations ensure that their CIO models are consistent with the business, technical, and cultural contexts of their enterprises. By defining mission improvement objectives, senior executives determine whether their organization needs a CIO who is a networking/marketing specialist, business change agent, operations specialist, policy/oversight manager, or any combination thereof.

In mid-June, OMB announced the establishment of an Associate Director for Information Technology and E-Government who will report to the Deputy Director for Management (the Deputy Director would act in the capacity of the federal CIO). According to the announcement from OMB, the Associate Director's responsibilities include (1) ensuring that the federal government takes maximum advantage of digital technology and best practices to improve quality, effectiveness, and efficiency, (2) leading the development and implementation of federal IT policy, and (3) directing the activities of the CIO Council. Since this is a new position, the specific authorities and duties of this official are unclear. For example, OMB's announcement stated that the Associate Director would be responsible for the e-government fund but was not specific as to whether this included, for instance, administering the fund and/or approving initiatives from agencies seeking to use the fund. It is also unclear how the Associate Director would relate to the Administrator of the Office of Information and Regulatory Affairs (OIRA) who has statutory information technology and

[63] GAO-01-376G, February 2001.

information resources management responsibilities under the Paperwork Reduction Act.

Your proposal, Mr. Chairman, would establish a federal CIO in statute. In this case, the federal CIO—appointed by the President and confirmed by the Senate—would report to the Director of OMB. The CIO would head a newly created Office of Information Policy and his or her responsibilities would include reviewing agency budget requests related to IT capital planning and investments, implementation of the Privacy Act, oversight of GPEA implementation, promulgation of federal information technology standards and guidelines, consultation with the General Services Administration on expenditures from its IT fund, and governmentwide statistical policy.

There are strengths associated with S. 803's federal CIO approach. Clearly, a single, central focus for information resources and technology management would exist in the federal government. A primary concern we have with OMB's 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 OIRA Administrator have other significant duties, which necessarily restrict the amount of attention that they can give to information resources and technology management issues.[64] A federal CIO, like agency CIOs, should be primarily concerned with information resources and technology management. Your bill would address this concern. Also, as the sole central focus for information resources and technology management, the federal CIO could be used to resolve potential conflicts stemming from conflicting perspectives or goals within the executive branch agencies.

Moreover, by positioning the federal CIO in OMB, the bill allows the CIO to leverage OMB's budget-review role in dealing with the agencies. 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.

Nevertheless, it is also important to note some potential challenges of having the CIO position located in OMB. Other legislative proposals have further elevated the visibility of the federal CIO by establishing a position

[64] While OMB's Director is responsible for these functions, they delegated to OIRA by the Paperwork Reduction Act. Under the Chief Financial Officers Act, the OIRA Administrator reports to the Director of OMB through the Deputy Director for Management.

that reports directly to the President and is also a Cabinet-level official.[65] 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.[66]

S. 803's federal CIO approach would also call for a delicate balancing act among the multiple areas requiring this individual's attention and involvement. In particular, the bill calls for the federal CIO to play a variety of roles in many of the bill's governmentwide initiatives, studies, and reports. For example, the bill calls on the federal CIO to (1) conduct a study and report on the feasibility of integrating federal information systems across agencies, (2) convene an interagency task force related to on-line access to federally funded research and development, (3) oversee the interagency initiative to develop common protocols for geographic information systems, (4) develop and establish a public domain directory of federal government Websites and post the directory on the Internet, and (5) promulgate standards and criteria for agency Web sites. Any one of these may be an appropriate role for the federal CIO, but they come coupled with the other functions specifically delegated to the CIO (such as the delegation of the OMB Director's responsibilities for the implementation of the Privacy Act) and the requirement that he or she be consulted on various issues. In order to fulfill such an ambitious agenda, the federal CIO will need to have sufficient and skilled staff and other available resources.

In addition to the establishment of a federal CIO, S. 803 contains many other important provisions. For example, the bill establishes 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 it. Moreover, as prime users of performance and financial information, having it statutorily based can help

[65] 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.

[66] GAO-01-376G, February 2001.

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 bill also (1) provides for a variety of measures that require using Internet-based IT to enhance citizen access to government information and services, (2) emphasizes the need to set and implement IT standards, and (3) authorizes that $650,750,000 be appropriated to carry out several of its provisions through fiscal year 2004 (the vast majority of these funds--$600 million—are earmarked for the bill's E-Government Fund).

In conclusion, e-government offers many opportunities to better serve the public, make government more efficient and effective, and reduce costs. The federal government is making strides in trying to take advantage of these opportunities although many of the more challenging initiatives are not yet implemented. As these move forward, a strong focus on the costs, benefits, and risks of the initiatives should be part of every decisionmaking forum. While there are many challenges that could serve as potential stumbling blocks if not overcome, such as privacy concerns, security, and the technology itself, these risks can be managed with effective leadership and management. A federal CIO—as called for by S. 803—could provide such needed leadership. Your bill takes constructive steps toward creating a federal CIO position that would address the many opportunities and challenges posed by the government's increasing foray into e-government.

Contacts and Acknowledgments

For information about this testimony, please contact me at (202) 512-6240 or by e-mail at *mcclured@gao.gov*. Individuals making key contributions to this testimony include John Christian, Felipe Colón, Jr., Lester Diamond, John de Ferrari, Norman Heyl, Linda Lambert, and Henry Sutanto.

Selected GAO Products Related to Electronic Commerce and Electronic Government

Electronic Commerce

Internet Pharmacies: Adding Disclosure Requirements Would Aid State and Federal Oversight (GAO-01-69, October 19, 2000)

Sales Taxes: Electronic Commerce Growth Presents Challenges; Revenue Losses Are Uncertain (GGD/OCE-00-165, June 30, 2000)

Commodity Exchange Act: Issues Related to the Regulation of Electronic Trading Systems (GGD-00-99, May 5, 2000)

Trade with the European Union: Recent Trends and Electronic Commerce Issues (GAO/T-NSIAD-00-46, October 13, 1999)

Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities (GAO/T-GGD-99-152, August 3, 1999)

Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities (GAO/GGD-99-91, July 6, 1999)

Securities Fraud: The Internet Poses Challenges to Regulators and Investors (GAO/T-GGD-99-34, March 22, 1999)

Retail Payments Issues: Experience with Electronic Check Presentment (GAO/GGD-98-145, July 14, 1998)

Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (GAO/GGD-98-100BR, May 1, 1998)

Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking (GAO/GGD-98-34, January 15, 1998)

Electronic Government – Agency-specific Initiatives

Computer-Based Patient Records: Better Planning and Oversight By VA, DOD, and IHS Would Enhance Health Data Sharing (GAO-01-459, April 30, 2001)

USDA Electronic Filing: Progress Made, But Central Leadership and Comprehensive Implementation Plan Needed (GAO-01-324, February 28, 2001)

Information Security: IRS Electronic Filing Systems (GAO-01-306, February 16, 2001)

U.S. Postal Service: Postal Activities and Laws Related to Electronic Commerce (GAO/GGD-00-188, September 7, 2000)

U.S. Postal Service: Electronic Commerce Activities and Legal Matters (GAO/T-GGD-00-195, September 7, 2000)

Defense Management: Electronic Commerce Implementation Strategy Can Be Improved (GAO/NSIAD-00-108, July 18, 2000)

Food Stamp Program: Better Use of Electronic Data Could Result in Disqualifying More Recipients Who Traffic Benefits (GAO/RCED-00-61, March 7, 2000)

National Archives: The Challenge of Electronic Records Management (GAO/T-GGD-00-24, October 20, 1999)

National Archives: Preserving Electronic Records in an Era of Rapidly Changing Technology (GAO/GGD-99-94, July 19, 1999)

Labor-Management Reporting and Disclosure: Status of Labor's Efforts to Develop Electronic Reporting and a Publicly Accessible Database (GAO/HEHS-99-63R, March 16, 1999)

Acquisition Reform: NASA's Internet Service Improves Access to Contracting Information (GAO/NSIAD-99-37, February 9, 1999)

Tax Administration: Increasing EFT Usage for Installment Agreements Could Benefit IRS (GAO/GGD-98-112, June 10, 1998)

Social Security Administration: Responses to Subcommittee Questions About the On-Line PEBES Service (GAO/AIMD-97-121R, June 20, 1997)

Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997)

Electronic Government - General

Electronic Government: Selected Agency Plans for Implementing the Government Paperwork Elimination Act (GAO-01-861T, June 21, 2001)

Information Management: Electronic Dissemination of Government Publications (GAO-01-428, March 30, 2001)

Information Management: Progress in Implementing the 1996 Electronic Freedom of Information Act Amendments (GAO-01-378, March 16, 2001)

Regulatory Management: Communication About Technology-Based Innovations Can Be Improved (GAO-01-232, February 12, 2001)

Electronic Government: Opportunities and Challenges Facing the FirstGov Web Gateway (GAO-01-87T, October 2, 2000)

Electronic Government: Government Paperwork Elimination Act Presents Challenges for Agencies (GAO/AIMD-00-282, September 15, 2000)

Internet: Federal Web-based Complaint Handling (GAO/AIMD-00-238R, July 7, 2000)

Federal Rulemaking: Agencies' Use of Information Technology to Facilitate Public Participation (GAO/GGD-00-135R, June 30, 2000)

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

Information Technology: Comments on Proposed OMB Guidance for Implementing the Government Paperwork Elimination Act (GAO/AIMD-99-228R, July 2, 1999)

Internet and Electronic Dial-Up Bulletin Boards: Information Reported by Federal Organizations (GAO/GGD-97-86, June 16, 1997)

World Wide Web Sites: Reported by Federal Organizations (GAO/GGD-97-86S, June 1, 1997)

Acquisition Reform: Obstacles to Implementing the Federal Acquisition Computer Network (GAO/NSIAD-97-26, January 3, 1997)

Electronic Signatures

Bank Regulators' Evaluation of Electronic Signature Systems (GAO-01-129R, November 8, 2000)

Electronic Signature: Sanction of the Department of State's System (GAO/AIMD-00-227R, July 10, 2000)

Corps of Engineers Electronic Signature System (GAO/AIMD-97-18R, November 19, 1996)

DOD's Reengineered Travel System Efforts (GAO/AIMD-96-62R, March 8, 1996)

Air Force Automated Travel System (GAO/AIMD-95-74R, February 14, 1995)

Electronic Imaging (GAO/AIMD-95-26R, November 10, 1994)

Treasury Electronic Signature Concept (GAO/AIMD-94-167R, August 11, 1994)

RCAS Authentication (GAO/AFMD-93-70R, May 4, 1993)

National Institute of Standards and Technology--Use of Electronic Data Interchange Technology to Create Valid Obligations (71 Comp. Gen. 109 (1991), December 13, 1991)

Internet

Telecommunications: Characteristics and Choices of Internet Users (GAO-01-345, February 16, 2001)

Telecommunications: Technological and Regulatory Factors Affecting Consumer Choice of Internet Providers (GAO-01-93, October 12, 2000)

Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers (GAO/OGC-00-33R, July 7, 2000)

Internet Census and Use Estimates (GAO/GGD-97-102R, May 12, 1997)

Information Superhighway: An Overview of Technology Challenges (GAO/AIMD-95-23, January 23, 1995)

Privacy

Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies" (GAO-01-424, April 27, 2001)

Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information (GAO-01-126SP, April 2001)

Internet Privacy: Federal Agency Use of Cookies (GAO-01-147R, October 20, 2000)

Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles (GAO-01-113T, October 11, 2000)

Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles (GAO/AIMD-00-296R, September 11, 2000)

Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy (GAO/GGD-00-191, September 5, 2000)

Social Security Numbers: Subcommittee Questions Concerning the Use of the Number for Purposes Not Related to Social Security (GAO/HEHS/AIMD-00-253R, July 7, 2000)

Security

Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk (GAO-01-600T, April 5, 2001)

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology (GAO-01-277, February 26, 2001)

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

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities (GAO/T-AIMD-00-181, May 18, 2000)

Information Security: Subcommittee Questions Concerning the Melissa Computer Virus (GAO/AIMD- 99-220R, June 18, 1999)

Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data (GAO/T-AIMD-99-146, April 15, 1999)

(310418)

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)