United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

September 2000

ELECTRONIC GOVERNMENT

Government Paperwork Elimination Act Presents Challenges for Agencies

GAO/AIMD-00-282

Contents

Abbreviations

ACES	Access Certificates for Electronic Services
CFO	chief financial officer
CIO	chief information officer
DNS	Domain Name System
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IT	information technology
ITAA	Information Technology Association of America
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	public key infrastructure
PRA	Paperwork Reduction Act
SSA	Social Security Administration
TCP/IP	Transmission Control Protocol/Internet Protocol

B-286007

September 15, 2000

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Dear Senator Lieberman:

Advances in the use of information technology and the Internet are transforming the way federal agencies communicate, use information, deliver services, and conduct business. If used effectively, these advances can help reshape government, making it more innovative, efficient, and responsive to the public. To increase the ability of citizens to interact with the federal government electronically, in 1998 the Congress enacted the Government Paperwork Elimination Act (P.L. No. 105-277, Div. C, tit. XVII). The act requires that by 2003 federal agencies provide the public, when practicable, the option of submitting, maintaining, and disclosing required information—such as employment records, tax forms, and loan applications—electronically, instead of on paper.

This report responds to your December 22, 1999, request for information regarding the (1) status of the Office of Management and Budget's (OMB) efforts to develop guidance implementing GPEA and (2) major challenges or impediments that might affect successful GPEA implementation.

Results in Brief

As required by GPEA, OMB has developed and issued useful guidance and procedures for implementing and reporting on GPEA efforts. In May 2000, OMB issued guidance describing key factors for agencies to consider in evaluating the practicability of giving persons or entities the option to electronically maintain, submit, or disclose required information, including the related use of electronic signatures. The guidance calls for agencies to examine business processes that might be revamped to employ electronic documents, forms, or transactions; identify customer needs and demands; consider the costs, benefits, and risks associated with making the transition to electronic environments; and develop plans and strategies for recordkeeping and security. The guidance requires each agency to develop and submit to OMB a GPEA implementation plan and schedule by

October 2000. In July 2000, OMB issued final reporting requirements for agencies to follow in preparing these plans and schedules.

In addition, OMB's May 2000 guidance directed several agencies to develop more detailed policies and guidance relevant to certain aspects of GPEA. In response, the Department of the Treasury has developed a policy paper on the use of electronic authentication techniques for federal payments, collections, and collateral transactions conducted over open networks; the National Archives and Records Administration (NARA) has developed guidance on managing records that have been created using electronic signature technology; the Department of Justice has drafted guidance on legal considerations in designing and implementing electronic processes; and the Department of Commerce's National Institute of Standards and Technology (NIST), in conjunction with the Federal Public Key Infrastructure (PKI) Steering Committee,[1] has drafted technical guidance on the use of public key technology for electronic signatures. At the close of our review in August 2000, final revisions were being made to these documents, and OMB expected them to be issued shortly.

While the guidance being developed will assist agencies in GPEA implementation, these documents alone will not ensure successful outcomes. Agencies' top management involvement, support, and leadership as well as diligent oversight from OMB and the Congress are essential. Moreover, agencies must address a variety of information technology (IT) management challenges that are fundamental to the success of GPEA. These issues, which agencies identified in comments or reports to OMB and in discussions with us, parallel IT management challenges identified in our past reviews of agencies' IT initiatives. Specifically, agencies will need to

- use disciplined investment management practices to ensure that the full costs of providing electronic filing, recordkeeping, and transactions prompted by GPEA are identified and examined within the context of expected benefits, such as lower transaction costs, increased productivity, and improved timeliness and quality of service delivery;
- adequately plan for and implement computer network and telecommunications infrastructures and technical architectures to

[1]The Federal PKI Steering Committee is a formal governmentwide committee that provides leadership, support, and coordination of agency activities to promote the development of an interoperable and extensible PKI.

provide the capacity and connectivity needed to support the electronic traffic generated by new or enhanced electronic offerings;
- provide a secure computing environment to support the broad array of e-government services envisioned by GPEA in order to reduce the risks of unauthorized access, which could lead to fraud, theft, destruction of assets, and service disruptions;
- develop adequate capabilities for creating, storing, retrieving, and, when appropriate, disposing of electronic records; and
- overcome two basic challenges related to IT human resources—a shortage of skilled IT workers and the need to provide a broad range of staff training and development—so that staff can effectively operate and maintain new e-government systems, adequately oversee related contractor support, and deliver responsive service to the public.

Appendix II lists recent GAO reports detailing these IT management problems.

Background

The dramatic rise in computer and network interconnectivity and interdependency in recent years has substantially changed how individuals, businesses, and government entities interact with one another. Business-to-business transactions, personal finance and banking, and travel and retail shopping are increasingly being done through the Internet and other means of electronic data exchange. According to a recent Department of Commerce report, the remarkable growth of the Internet in recent years shows no signs of abating. During the past year Internet access has grown significantly in all regions of the world, rising from 171 million people in March 1999 to 304 million in March 2000. The amount of information available to people with Internet access has also grown rapidly. A recent study indicates that in January 2000 the World Wide Web contained more than 1 billion unique pages, compared to 100 million in October 1997. Moreover, according to a summary prepared by *The Industry Standard,* forecasts for 2003 of the dollar value of transactions that are conducted electronically between U.S. businesses range from $634 billion to $2.8 trillion.[2]

Government agencies have implemented an array of e-government applications including using the Internet to collect and disseminate all

[2]*Digital Economy 2000,* June 2000, Department of Commerce.

types of information and forms; buy and pay for goods and services; enable citizens to file claims and comments or ask questions; submit bids and proposals; order records; and apply for licenses, grants, and benefits. For example, the General Services Administration, the National Aeronautics and Space Administration, the Department of Defense, and other agencies have been implementing on-line procurement operations for several years and are expanding their use of electronic commerce to facilitate day-to-day operations. Similarly, the Internal Revenue Service, Department of Education, and Social Security Administration have been using Internet applications to improve service delivery to taxpayers, students, and senior citizens.

GPEA promotes expansion of this trend. Specifically, GPEA requires federal executive agencies by 2003 to provide individuals or entities that deal with agencies the option of electronic maintenance, submission, or disclosure of information, as a substitute for paper, including the related use of electronic signatures when practicable. These options will in some cases replace and in others supplement existing paper processes. The act encourages electronic filing and electronic recordkeeping, particularly by employers, and gives electronic records and their related electronic signatures full legal effect. It also requires agencies to guard privacy and protect documents from being altered and encourages federal government use of a range of electronic signature alternatives. The recently enacted Electronic Signatures in Global and National Commerce Act (P.L. 106-229) complements GPEA in that it gives legal validity and enforceability within the United States to the use of electronic records and signatures in interstate and foreign commerce.

In order to undertake the electronic information processes contemplated by GPEA, the use of electronic signatures becomes increasingly important. Electronic signatures are a key element of many electronic transactions. GPEA defines an electronic signature as a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message and indicates such person's approval of the information contained in the electronic message. Several techniques can be used to produce electronic signatures. One type is a digital signature which relies on cryptographic techniques to help ensure data integrity

Implementing GPEA effectively will require agencies to consider the existing framework of laws, directives, and guidance intended to improve the federal government's ability to use IT effectively and securely as a means to reduce costs and improve service. This framework includes the

Paperwork Reduction Act; the Clinger-Cohen Act; the Computer Security Act; OMB Circular A-130, *Management of Federal Information Resources,* which provides uniform governmentwide information resources management policies including those related to performance measurement, strategic planning, information systems management oversight, and information security; OMB's Memorandum M-97-02, which establishes the decision criteria that OMB will use to evaluate major information system investments proposed for submission in the President's Budget; OMB's Memorandum M-00-07, which requires agencies to explicitly identify how they are building security into system architectures; and GAO's guides on business process reengineering, information security management, and information technology investment management. A list of GAO guides is provided in appendix III.

OMB Has Issued GPEA Implementation Guidance

GPEA states that OMB is responsible for ensuring that federal agencies meet GPEA's October 21, 2003, implementation deadline to give persons or entities who are required to maintain, submit, or disclose information the option of doing so electronically when practicable. To help accomplish this, GPEA directs OMB to develop procedures for federal agencies to follow in using and accepting electronic signatures and for allowing private employers to store and file electronically with executive agencies forms containing employee information.

On May 2, 2000, OMB issued GPEA implementation guidance, which lays out a process and principles for agencies to employ in evaluating the use and acceptance of electronic documents and signatures.[3] The OMB guidance is in two parts. The first part sets forth the policies and procedures agencies should follow to implement the act. The second part is intended to provide federal managers with guidance on deciding whether to use electronic signature technology for a particular application. Overall, the guidance directs agencies to develop and implement plans for optional electronic filing and recordkeeping. These plans must be supported by an assessment of the practicability of submitting information electronically, maintaining records electronically, and using electronic signature technologies. Figure 1 highlights major steps that agencies are to take in doing so.

[3]On March 5, 1999, OMB published proposed GPEA implementation guidance for public comment in the *Federal Register* (64 FR 10896). It was also sent directly to federal agencies for comment and made available through the Internet.

Figure 1: Steps Outlined in OMB Guidance to Agencies for Implementing GPEA

1. Examine business processes that might be revamped to employ electronic documents, forms, or transactions.
2. Identify customer needs and demands as well as the existing risks associated with fraud, error, or misuse.
3. Identify the benefits and risks that may accrue from the use of electronic transactions or documents.
4. Study the legal implications about the use of electronic transactions or documents in the particular application.
5. Evaluate electronic signature alternatives, including risks, costs, and practicality.
6. Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who need it.
7. Develop management strategies to provide appropriate security for physical access to electronic records.
8. Determine whether regulations and policies are adequate to support electronic transactions and recordkeeping or additional agreements are needed for the particular application.
9. Integrate these plans into the agency's strategic IT planning and regular reporting to OMB.

To assist in monitoring agencies' efforts to implement GPEA and transition to e-government, OMB's guidance requires each agency, by October 2000, to develop and submit to OMB a GPEA implementation plan and schedule. According to OMB, the plan should prioritize implementation of systems or system modules based on achievability and net benefit. Agencies must coordinate the GPEA plan and schedule with their strategic IT planning activities and must report progress annually. Agencies' GPEA progress reporting should be consistent with and incorporated into annual performance reporting required under OMB Circular A-11, *Preparation and Submission of Budget Estimates.*

In July 2000, OMB issued procedural guidance to further explain reporting requirements for agency GPEA implementation plans and provide more structured and standardized report formats. The reporting guidance requires agencies to submit information regarding plans for providing a

fully electronic option for transactions that are part of the agency information collection activities under the Paperwork Reduction Act (PRA)[4] as well as other transactions, such as interagency reporting and information dissemination activities. The guidance defines a fully electronic option as one that requires no compulsory paper-based reporting, signatures, correspondence, or dissemination to or with the respondents. An agency must provide OMB with an explanation if it determines that optional electronic reporting to or communication with respondents is not practicable.

The guidance outlines the content and format of the plan, provides examples of the types of transactions covered by GPEA, and reiterates the requirement from the May guidance that an agency's GPEA plan relate to strategic IT planning in the budget process. Specifically, if an agency needs additional resources to implement the plan, its budget request under OMB Circular A-11 should reflect that need, and agency Government Performance and Results Act reports should address, as appropriate, progress in implementing GPEA and e-government initiatives.

In addition, OMB is providing each agency a list of the agency's information collections that already allow for at least some electronic reporting. OMB is obtaining this information from a database that it maintains on current information collections. Agencies are to review this list for accuracy and use it to determine which of the collections provide a fully electronic option. According to OMB, this list of collections, along with the standard reporting formats for GPEA, should assist agencies in developing GPEA plans and provide standard, baseline information for the agencies and OMB to use in monitoring the progress of GPEA implementation and the transition to e-government. OMB officials told us that a primary means of providing continuing guidance and oversight for the implementation of GPEA will be its review and annual reporting of agencies' information collection activities.

OMB's reporting guidance requires an agency's GPEA submission to include the following information:

[4]The Paperwork Reduction Act of 1995 (P.L. 104-13) gives OMB certain responsibilities for overseeing federal information collection. OMB reviews agencies' information collections to determine why they need the information, how they plan to use it, and whether there is a better way to collect it.

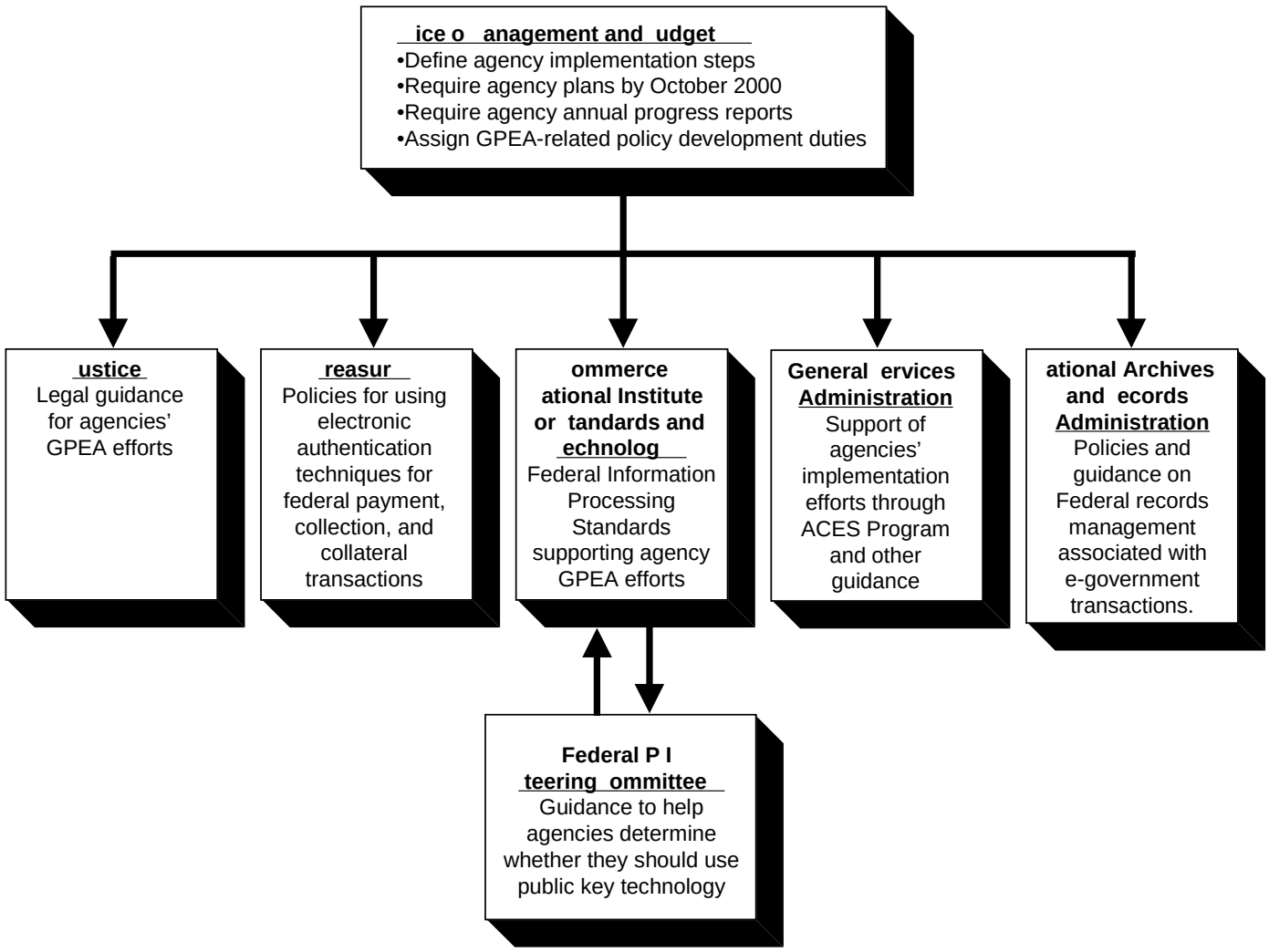
- a cover letter describing the agency's overall strategy and efforts to comply with GPEA and meet its deadlines;
- an agency's plans for offering a fully electronic option for transactions that are part of information collections covered by the PRA reporting process as well as interagency reporting and information dissemination activities with estimates, for each collection or report, of the number of persons or entities involved, the date for offering a fully electronic option, and plans for using electronic signatures;
- for any transactions that an agency has determined pose a "high risk," such as those that involve particularly sensitive information collections or very large numbers of respondents, additional information describing the transaction, its sensitivity, and additional risk management measures that will be undertaken.

Agency GPEA plans and schedules are due to OMB no later than October 31, 2000. Annual progress reports and updates to an agency's GPEA plan and schedule will be submitted to OMB for review as part of the annual reporting required under the PRA and the OMB Circular A-11 process.

Other Federal Agencies Are Developing Related GPEA Guidance

In addition to guidance on developing agency implementation plans, OMB's GPEA guidance assigns more specific responsibilities to five other agencies. These responsibilities pertain to providing supplemental policy, practical guidance, or support to agencies in specific areas related to GPEA goals and implementation, including electronic records management; legal considerations; and the implementation of authentication technologies, including digital signatures.

Figure 2: Federal Entities Involved in Establishing Governmentwide GPEA Guidance



These entities have already either begun support efforts or drafted guidance. OMB is currently reviewing all the draft supplemental guidance documents to ensure that discussions of similar topics, such as risk management, are appropriately consistent and not overly duplicative. Upon final approval by OMB, these guidance documents will be issued in final form. The status of each of these efforts is described below.

- The Department of the Treasury has developed a policy paper on the use of electronic authentication techniques, including digital signatures, for federal payment, collection, and collateral transactions conducted over open networks, such as the Internet. In general, the paper describes the importance of assessing risk factors, such as monetary loss, reputation risk, and productivity risk for each program or system under consideration in order to determine robustness of the electronic authentication techniques that must be used. Treasury sent a draft policy paper to OMB and other agencies for review on March 15, 2000. Treasury officials told us that they revised the policy paper based on agency comments.
- The National Archives and Records Administration (NARA) has developed guidance on managing records that have been created using electronic signature technology. Among other matters, this guidance, which is intended to supplement existing NARA guidance on records management, discusses various approaches available to ensure the trustworthiness of electronically signed records, including records that need to be preserved for a finite period of time or permanently; how agencies can determine which electronic signature records to retain; and special considerations for records documenting legal rights and records that must be retained permanently. NARA provided draft guidance to OMB and other agencies for review on April 7, 2000. NARA officials told us that they made further revisions to the document based on comments received from agencies.
- The Department of Justice has drafted a detailed guide for federal agencies on legal considerations in designing and implementing electronic processes. The Justice guide explains the legal implications associated with implementing electronically based processes, examines four overarching issues (accessibility, legal sufficiency, reliability, and legality) that should be considered in deciding whether and how to convert any given type of system or operation, and discusses general and specific steps agencies should consider in converting to electronic processes. The guidance, which was provided to OMB and other agencies for comment on May 3, 2000, refers agencies to guidance issued by OMB and NARA, and recommends that agencies use available sources of expertise, such as the agency's general counsel and inspector general's office, to reduce the legal risks of "going paperless." Justice is now revising the draft guidance based on comments received.

- The Department of Commerce's NIST and the Federal PKI Steering Committee have drafted technical guidance to assist federal agency officials in determining when to use public key technology for digital signatures or authentication over open networks such as the Internet. A PKI is a system of computers, software, policies, and people that can be used to facilitate the protection of sensitive information and communications.[5] The draft guidance includes specific questions and issues that agencies should consider in evaluating potential applications of public key technology for digital signatures and user authentication and in properly implementing those applications selected. In addition, the guidance states that implementation of digital signatures may necessitate the transformation of business processes. The steering committee sent out the document for agency review and comment on May 30, 2000. The steering committee revised the document based on agency comments and submitted it to OMB in early July 2000. The Chair of the steering committee told us that the document has subsequently been provided to NIST. It will be issued as a "Special Publication" upon final approval by OMB.
- The OMB GPEA guidance tasks the General Services Administration (GSA) to support agencies' implementation of digital signature technology and related electronic service delivery. GSA has been working since 1996 on a program called Access Certificates for Electronic Services (ACES), which is intended to help jumpstart agency adoption of PKI technology by providing agencies a range of support services so that individual agencies will not have to design and build their own PKIs. In 1999, GSA awarded an ACES contract for these services to three vendors. In May 2000, GSA arranged with two of these vendors to make 500,000 ACES certificates available for use free of issuance cost. GSA and the contractors hope that by waiving the issuance cost of certificates, federal agencies will be motivated to use ACES to provide businesses and the public with a safe and secure way to interact with the government over the Internet. The PKI Steering Committee guidance discussed in the previous paragraph encourages agencies to consider using ACES contracts. However, agencies are free

[5]For more information on public key technology, see *The Evolving Federal Public Key Infrastructure* (Federal Public Key Infrastructure Steering Committee, Federal Chief Information Officers Council, June 2000), gits-sec.treas.gov; and *Information Superhighway: An Overview of Technology Challenges* (GAO/AIMD-95-23, January 23, 1995).

to pursue their own PKI vendor services through agency-specific contract vehicles if they wish.[6]

The OMB GPEA guidance also tasked NIST to develop Federal Information Processing Standards (FIPS), as appropriate, to further the goals of GPEA. Although NIST believes that current FIPS are sufficient to cover GPEA requirements, the agency is working on enhanced security standards and is open to considering agencies' proposals for additional FIPS where a need is not being met by current FIPS or voluntary industry consensus standards.

The Treasury, NARA, Justice, and NIST documents will provide guidance on the issues they address to supplement the broader OMB guidelines on GPEA implementation. Agencies can refer to these documents in preparing their GPEA plans to ensure that they are giving adequate consideration to key implementation issues covered by the act.

Challenges in Implementing GPEA

As agencies respond to GPEA, the new technology applications and opportunities that result will undoubtedly continue to change the way the federal government conducts business, communicates, and interacts with citizens, industry, and other government entities. Nevertheless, in comments on a draft of OMB's guidance and in comments on their own e-government initiatives, agencies have identified several issues as significant challenges to successfully implementing the types of electronic services envisioned in GPEA. These challenges parallel concerns that we have raised in previous reports on agencies' IT initiatives (see appendix II). Specifically, agencies noted the challenges of identifying and providing for the full costs associated with electronic forms processing and other transactions; ensuring the adequacy of computer technology infrastructures that are to be used for e-government services; ensuring the security and privacy of electronic transactions; overcoming recordkeeping challenges; and acquiring skilled employees and providing appropriate training.

None of these challenges is insurmountable, but they must be addressed at the program, agency, and governmentwide levels to ensure successful e-government outcomes. In addition, overcoming these challenges will require effective leadership by agencies' chief information officers (CIO)

[6]For more information on ACES, see GSA's Web site at: www.gsa.gov/aces/.

working in partnership with the program organizations. The information technology reforms now required by the Congress, including GPEA, will be difficult for agencies to achieve without effective CIO leadership in place to ensure that IT investment decisions are directly integrated into the agencies' strategic and program plans. As we recently testified, while notable progress has been made in establishing federal CIOs, more remains to be done to ensure that these executives establish themselves as effective information management leaders, build credible information management organizations, and deliver high-value IT investment results. [7]

The Importance of Sound IT Investment Decision-Making Practices

E-government is dependent on the effective use and management of information technologies. A primary challenge for agencies in moving toward e-government is to implement and follow information technology 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.

Several agencies emphasized that GPEA-related initiatives will be costly to implement. They expressed concern about securing funds for the many efforts involved, such as updating network plans, conducting risk analyses, evaluating technology alternatives, procuring and installing recordkeeping software, and testing networks. The Social Security Administration (SSA) noted in comments on OMB's initial draft guidance for GPEA implementation that implementing GPEA could cost SSA over $40 million and run past the year 2005 if SSA were to include full electronic processing of transactions in its efforts. Because GPEA requires agencies to add the option of transmitting forms and services electronically when practicable, while preserving the paper-driven processes already in place, the legislation entails extra expenses, at least in the short term.

Careful IT investment planning will be critical as agencies determine which GPEA projects to fund. Many of our agency information technology management assessments have identified fundamental weaknesses in the way information technology investment decisions are made, including (1) a lack of clarity about how these investments are being or will be used to improve performance or help achieve specific agency goals and (2) incomplete data on which to base informed decisions. Moreover, our

[7] *Chief Information Officers: Implementing Effective CIO Organizations* (GAO/T-AIMD-00-128, March 24, 2000).

reviews of strategic plans and annual performance plans have noted weak linkages between the mission goals and planned or ongoing information technology initiatives that are essential to achieving those goals.[8]

While GPEA focuses on the need to develop and offer electronic options for forms and services, it also links directly to mission performance outcomes. Electronic delivery, authentication, and processing of forms and services will, in many instances, require agencies to consider additional organizational changes to accommodate new ways of doing business. These changes may be time consuming and could delay agencies' progress toward meeting GPEA goals. For instance, the Food and Drug Administration, in its comments to OMB's draft GPEA guidance, stated that an electronic environment requires a "paradigm shift" to a new way of doing business and requires additional resources and planning efforts to train agency personnel for this new corporate culture. Treasury officials observed that customer expectations will be a force for change because electronic transactions create an expectation on the part of users that they will get quick responses. This new way of operating will create training needs and may necessitate fewer layers of review within agencies.

Addressing these issues will require agencies to implement a disciplined approach to investment management. Without such an approach, IT projects can become risky, costly, unproductive mistakes. There are some governmentwide efforts on these issues underway. For example, during the summer of 2000, OMB is meeting with all CIO Council agencies regarding their IT capital planning and investment control processes. The meetings are between the CIO, chief financial officer (CFO), the procurement executive, and budget officer of each agency and the OMB statutory offices and resource management offices. According to OMB officials, these meetings will result in agency guidance for the fiscal year 2002 budget submission and for improving their investment management processes overall.

The Need for Adequate Systems Architectures and Technology Infrastructures

Information technology initiatives, including e-government programs, require well-designed, robust systems architectures. Agencies evaluating the capabilities of their current information systems may find that they will have to make extensive changes to their technical architectures to meet the

[8] *Managing for Results: Opportunities for Continued Improvements in Agencies' Performance Plans* (GAO/GGD/AIMD-99-215, July 20, 1999).

requirements of GPEA. Our reviews show that agencies often attempt to build modernized systems before having complete and enforced enterprise architectures. These architectures are essentially construction plans that systematically detail the full breadth and depth of an organization's mission-based mode of operations in logical and technical terms. Without these blueprints to guide and constrain IT investments, such as interdependent e-government system applications, there is no systematic way to preclude either inconsistent system design or inconsistent development decisions and the resulting suboptimal performance and added cost associated with incompatible systems.[9]

Success in e-government also will require an adequate technology infrastructure, such as the telecommunications networks, databases, hardware, interfaces, and operating software that will support easy and reliable electronic access to government. In comments to OMB and in discussions with us, many agencies expressed concern that in going forward with GPEA implementation, upgrades or improvements in agencies' computer network infrastructures may be needed. In particular, attention may be needed in the following areas.

- *Providing adequate network capacity or bandwidth.* Government agencies will need to consider the amount of electronic traffic that will be generated by an electronic offering and provide adequate connectivity to support that load. Some Web sites have been completely overwhelmed and disabled when far greater numbers of users visited the sites than their developers had anticipated. In 1997, realizing that Web pages for its Mars Pathfinder mission might be overloaded by large numbers of visitors from around the world, NASA was able to circumvent such an overload by setting up mirror (duplicate) sites to handle these visitors.
- *Ensuring the reliability of platform and software applications.* As GPEA implementation progresses, agencies will increasingly depend on computers and telecommunications to perform important functions that are essential to the national welfare and that directly affect the lives of millions of people every day. Such functions are likely to support critical

[9]For discussions of the importance of systems architecture, see GAO's Performance and Accountability Series, *Major Management Challenges and Program Risks: A Governmentwide Perspective* (GAO/OCG-99-1, January 1999); *Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization* (GAO/AIMD-97-30, February 3, 1997), and *Customs Service Modernization: Architecture Must Be Complete and Enforced to Effectively Build and Maintain Systems* (GAO/AIMD-98-70, May 5, 1998).

operations related to national defense, tax collection, import control, benefits payments, and law enforcement—operations that must not be subject to frequent disruptions or slowdowns. The Web servers and other computer platforms that support e-government services—including their operating systems and the software that connects them—must provide reliable support for potentially heavy user demands. Systems must reliably confirm that a transaction is complete and also must reliably abort a transaction completely and consistently in the event that a problem occurs. The technology in use today does not always respond consistently and unambiguously.

- *Developing common technical standards.* Even a smoothly operating electronic delivery service will fail to fulfill the promise of e-government if users cannot use it easily. The use of common technical standards will help. For example, basic functions such as browsing an on-line catalog and placing an order rely on the TCP/IP (Transmission Control Protocol/Internet Protocol) for the transmission of data over the Internet, DNS (Domain Name System) for translating computer names into numeric IP addresses, HTTP (Hypertext Transfer Protocol) for information exchange between the Web browser and Web server, and HTML (Hypertext Markup Language) for formatting Web content. Besides these well-established and widely used standards, other standards are being developed to provide interoperable electronic delivery of services to the public.

To help agencies with many of these issues, the Federal CIO Council, with assistance from GAO, is developing a guide to provide a suggested framework to agencies as they carry out the processes necessary to develop and maintain an enterprise architecture. This guide builds on policy guidance that began in 1997 with OMB's Memorandum M-97-16, *Information Technology Architectures,* which establishes the minimum criteria for IT architecture required of agencies by the Clinger-Cohen Act of 1996. In September 1999, the CIO Council issued the Federal Enterprise Architecture Framework to provide an organized structure and common terms for federal entities to use in developing within their own organizations specific architectures that could then be integrated with governmentwide systems.

Ensuring Security and Privacy

A secure computing environment will be needed to support the broad array of e-government services envisioned by GPEA. Participants—including government agencies, private businesses, and individual citizens—must feel comfortable using electronic means to carry out sensitive transactions,

such as obtaining a license, bidding on a contract, or making a benefit claim. Personal information must be adequately protected from unauthorized disclosure, and electronic transactions must be guarded against tampering and fraud. Also, essential computer systems must be protected from undue disruptions, such as those resulting from recent computer virus epidemics.[10]

Establishing an adequately secure computer environment will be a major undertaking for federal agencies because most have not institutionalized basic controls and management practices to effectively manage computer security risks. The Department of Transportation, in its comments on OMB's proposed GPEA implementation guidance, underscored the need for improved security, stating that "opening databases creates potential vulnerabilities, including those related to security administration, key management, and system configuration."

Concerns about security needs for GPEA initiatives reflect security concerns about computerized federal operations in general. Audit reports that we and agency inspectors general have issued have identified serious and pervasive computer security weaknesses throughout the federal government. Our most recent analysis showed that such weaknesses were reported for 24 of the largest federal agencies from July 1999 through August 2000.[11] Repeatedly, we have found that the underlying cause of these persistent problems is that agencies have not instituted a basic cycle of management procedures for ensuring that risks are fully understood and that controls implemented to mitigate risks are effective. For example, since July 30, 1999, we have reported such weaknesses at the departments of Energy, Treasury, Defense, and Agriculture, and at the Environmental

[10]For information on recent computer virus epidemics see *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); *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000); and *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000).

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

Protection Agency.[12] While agencies are working to correct specific control deficiencies as well as the related management weaknesses, progress has been slow. We, in our comments on OMB's proposed GPEA implementation guidance, emphasized that agencies need to perform careful risk assessments before implementing GPEA.[13]

As with other aspects of GPEA, addressing security and privacy needs is likely to require additional funding—at least in the short term—as agencies make investments in the infrastructure and capabilities needed to enable secure electronic business operations. Agencies have been required to secure critical and sensitive data for decades. In particular, the Computer Security Act of 1987 and related OMB guidance have required agencies to assess their information security risks and implement security controls commensurate with these risks. Nevertheless, agencies noted that they may be hard-pressed to allocate sufficient resources to provide the level of assurance necessary for widespread implementation of electronic federal processes. For example, the Department of Agriculture, in commenting on OMB's proposed GPEA implementation guidance, noted that it would have to update its network plans, conduct risk analyses, evaluate technology alternatives, and perform network testing, and that the requisite funding and staff resources were not available for the immediate future.

In addition to improvements at individual agencies, a more effective governmentwide strategy for improving federal security is needed to fully realize the benefits of GPEA implementation—a strategy that involves conducting routine periodic independent audits of agency security programs; assisting agencies in determining the level of protection that is appropriate for various types of data under their control; and strengthening central leadership and coordination of information security–related activities across government. As we testified in July 2000, an important

[12] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000); *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/T-AIMD-00-97, February 17, 2000); *Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-4, October 4, 1999); *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999); *Bureau of the Public Debt: Areas for Improvement in Computer Controls* (GAO/AIMD-99-242, August 6, 1999); *USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-99-227, July 30,1999).

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

element of such efforts will be defining and clarifying the roles and responsibilities of organizations—especially federal entities—serving as central repositories of information or as coordination focal points.[14] For example, the disruption caused by the recent ILOVEYOU virus attack in May 2000 illustrated that the federal government, as well as other government and industry sectors, were not effective in detecting viruses early and immediately warning agencies about the imminent threat.[15] Federal entities with governmentwide responsibilities—including OMB, the CIO Council, the Federal Computer Incident Response Capability, and the National Infrastructure Protection Center—are currently working with federal agencies to improve our government's ability to share critical information and respond to events such as the ILOVEYOU attack. In addition, they have initiated several efforts to assist agencies in fundamentally improving their information security programs, including development of a common framework for evaluating agency progress in this area.

Another important element of security will be wider implementation of public key cryptography. Such technology, when properly implemented and maintained, can provide assurance that (1) the parties to an electronic transaction are really the entities they claim to be, (2) information has not been altered, and (3) neither party will be able to wrongfully deny that they took part in the transaction when acknowledgments are used. Key federal security experts believe that these assurances are necessary to support broader implementation of e-government services.

The federal government is aggressively promoting the deployment of PKI technology. The Federal PKI Steering Committee, for example, was established to coordinate PKI pilot projects on a governmentwide basis and to undertake efforts to encourage the adoption of PKI technology. Federal agencies—including NASA, DOD, and the Patent and Trademark Office—are experimenting with 24 pilot PKI programs. Furthermore, as mentioned earlier, GSA's ACES program is intended to facilitate agency adoption of PKI technology by establishing a framework for issuing and managing digital signature certificates.

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

[15]GAO/T-AIMD-00-181, May 18, 2000, and GAO/T-AIMD-00-171, May 10, 2000.

The public key and digital signature technologies used to authenticate sensitive electronic transactions are a source of concern that some agencies mentioned in comments on OMB's draft GPEA guidance. Our own work indicates that these technologies will require further development.[16] A number of significant challenges must still be overcome before the technology can be widely deployed and implemented in the federal government. For instance, it has not yet been demonstrated that a governmentwide federal PKI, connecting hundreds of thousands or millions of users, can operate efficiently and effectively. The government is developing a Federal Bridge Certification Authority (FBCA) to serve as electronic "glue" to connect the various PKIs that are developed separately by different federal agencies. Although a prototype test involving five organizations' PKIs was conducted in April 2000, the FBCA is not yet operational and not all of its functions have yet been demonstrated. In addition, a significant up-front cost is involved in fielding and maintaining PKI capability. Certification authorities, including those established by the ACES program, must be set up to positively identify users, issue them electronic certificates, and manage the exchange, verification, and revocation of certificates. In addition, existing software and systems must be modified so that they can interact with the PKI. Lastly, although several PKI products are currently on the market, many believe that interoperability and user friendliness could be improved.

Establishing Reliable Recordkeeping

In implementing GPEA and moving toward e-government, executive-branch agencies and 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. Staff members creating records, for example, need to be made aware of what constitutes an electronic record, how to save it, and how to archive it for future use. For e-mail alone, this can be an intricate task given the (1) huge volumes of e-mail agency employees now send and receive in performing their official duties and (2) related privacy issues.

When deciding how to store electronic documents, agencies must take into account the legal viability of the records they create. The Department of Justice, in its draft guidance for federal agencies on designing and implementing electronic processes, notes that agencies must ensure that

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

the important information in a transaction is collected, retained, and accessible whenever needed, even years later, and even when changes have occurred to computer hardware and software. These records must be sufficiently reliable and persuasive to satisfy courts and others who must assess agency actions. In addition, agencies' use of electronic methods to obtain, send, disclose, and store information must comply with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility for disabled individuals.

The long-term preservation and retention of those electronic records is a challenge because software products change frequently. The Department of Health and Human Services, in its comments on OMB's initial draft guidance for GPEA, expressed concerns about obsolescence of hardware and software, and NARA, in its guidance, remarked that this obsolescence can make record retention burdensome. The NARA guidance developed in response to GPEA also 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 at the agencies. The guidance points out that in systems implemented as a result of GPEA, records management requirements will be an important element of the IT system requirements.

NARA itself must be able to receive electronic records from agencies, store them, and retrieve them when needed.[17] To do so, it must expand its capacity to accept an increasing volume of electronic records from agencies. NARA notes that federal agencies are individually generating huge volumes of electronic records annually just in e-mail, much of which may need to be preserved by NARA. In addition to the increasing volume, the increasing variety of electronic records such as word processing documents, e-mail messages, databases, digital images, and Web site pages complicate NARA's mission to preserve these records. According to NARA, it lacks the capacity to accommodate its current backlog of files and the exploding volume and variety of electronic data files that it receives from federal agencies.

[17]For further information on NARA's activities, see *National Archives: Preserving Electronic Records in an Era of Rapidly Changing Technology* (GAO/GGD-99-94, July 19, 1999).

Providing Expertise and Training

As federal agencies increase their efforts to provide electronic service delivery systems, they face a short supply of IT human resources to develop and manage Web-based and other applications that will be required to implement GPEA. The demand for IT workers is large and growing. According to an April 2000 skills study by the Information Technology Association of America (ITAA), employers will attempt to fill 1.6 million new IT jobs in 2000. The largest skill gaps are for enterprise systems integration and Web development positions. These positions require advanced technical skills, and qualified applicants are scarce. Technical support and network administration positions, requiring skills in troubleshooting, customer service, and systems operations and maintenance, also are in high demand by both IT and non-IT companies.

In a 1999 survey conducted by ITAA, federal CIOs reported that IT workforce issues, including age, skill mix, and recruiting problems, are becoming the most vexing problems confronting them. For example, several CIOs indicated that over 50 percent of their IT workforce would be eligible to retire within 3 years, underscoring the workforce issue as a problem that would get worse before it gets better. The rapid rate of technological change, in combination with the lack of current technological skills, is creating a significant gap between skill supply and demand in the federal workplace. CIOs also reported a lack of more traditional skills—project and program management and contract management skills.

The Federal CIO Council has recognized increasing difficulties that agencies have in recruiting qualified staff. Federal salaries and benefits are perceived as less competitive with each passing year. The council is working to validate and substantiate the extent of the federal IT workforce challenge and to develop and implement strategies for recruitment, retention, and development of IT professionals.

In addition to recruiting qualified staff, implementing GPEA will require staff training in a number of areas. Agencies are becoming acutely aware that e-government technology applications work only if people have the training to execute them properly. Increasing the computer literacy of the federal workforce can help to ensure that, as citizen-to-government interactions become more automated, government employees are ready to actively participate in the transition. The new technology also creates a need for specialized training of available staff in areas such as Web-based applications, security, and software maintenance and engineering.

In particular, 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. Training is especially important in making the transition to applications called for by GPEA because these applications demand that organizations move away from a paper-based business paradigm to an electronic, customer-centric paradigm. In comments on OMB's initial draft guidance for implementing GPEA, agencies expressed concerns about the training that will be required, noting that such training will entail time and expense. The Department of Agriculture, for example, commented in its response to OMB's initial draft guidance that implementing GPEA would lead to significant changes in the way federal agencies currently operate, and Agriculture would have to train both its employees and its customers to do business differently.

Conclusions

OMB's guidance—as well as the guidance and supplementary efforts being undertaken by Treasury, NARA, Justice, Commerce, the Federal PKI Steering Committee, and others—provides a useful foundation of information to assist agencies with GPEA implementation and the transition to e-government. Effectively applying the guidance will require agencies to undertake significant planning and training efforts and to devote time and attention to intra-agency and governmentwide implementation and coordination issues. In doing this, agencies must overcome the challenges that have historically troubled many information technology initiatives: poorly planned and implemented investment practices, inadequate technology infrastructures, insufficient security and privacy measures, changing recordkeeping needs and technologies, and gaps in technical expertise and training.

Effective GPEA implementation will depend on top agency leaders, OMB, and the Congress ensuring that steps toward e-government are effectively merged with corresponding management and process improvements. This oversight will be critical in ensuring that agencies work efficiently within a changing technological environment while applying the varied and evolving guidance provided by OMB and other federal entities. Agency and congressional leaders will have to provide sustained direction and oversight as well to overcome the challenges that accompany—and can derail—information technology initiatives.

As previously mentioned, issues we have covered in prior reports provide an overview of the types of challenges that agencies will need to address to maximize the opportunities for successful GPEA implementation. Our previous reports, listed in appendix II, contain recommendations to agencies for improving their IT management practices. In addition, GAO has published guidance on several of these issues that agencies can refer to when planning their GPEA initiatives. This guidance is listed in appendix III.

Agency Comments and Our Evaluation

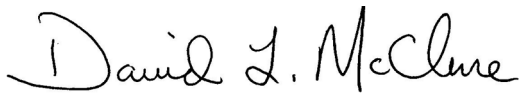
In oral comments on a draft of this report, officials from OMB's Office of Information and Regulatory Affairs generally agreed with the information presented regarding OMB's efforts to develop guidance implementing GPEA and the discussion of major challenges to successful GPEA implementation. They offered comments of a technical or clarifying nature, which we have incorporated where appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its issue date. At that time, we will send copies to Senator Fred Thompson, Chairman, Senate Committee on Governmental Affairs; Senator George V. Voinovich, Chairman, and Senator Richard J. Durbin, Ranking Minority Member, Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia, Senate Committee on Governmental Affairs; Senator Jon Kyl, Chairman, and Senator Dianne Feinstein, Ranking Minority Member, Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary; Senator Christopher S. Bond, Chairman, and Senator John F. Kerry, Ranking Minority Member, Senate Committee on Small Business; Representative Tom Bliley, Chairman, and Representative John D. Dingell, Ranking Minority Member, House Committee on Commerce; Representative Steve Horn, Chairman, and Representative Jim Turner, Ranking Minority Member, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform; Representative Constance A. Morella, Chairwoman, and Representative James A. Barcia, Ranking Minority Member, Subcommittee on Technology, House Committee on Science; and Representative Jim M. Talent, Chairman, and Representative Nydia M. Velazquez, Ranking Minority Member, House Committee on Small Business. In addition, we are providing copies to the Honorable Jacob J. Lew, Director, Office of Management and Budget, and

other interested parties. Copies will be made available to others upon request.

If you have questions regarding this report, please contact me at (202) 512-6240 or by e-mail at *mcclured.aimd@gao.gov.* Key contributors to this report were Jean Boltz, Cristina Chaplain, Mary Marshall, and Pat Slocum.

Sincerely yours,



David L. McClure
Associate Director
Defense and Governmentwide
Information Systems

Objectives, Scope, and Methodology

Our objectives were to determine (1) the status of the Office of Management and Budget's (OMB) efforts to develop guidance for executive agencies on implementing GPEA, and (2) major challenges or impediments that might affect GPEA implementation.

To determine the status of OMB's efforts to develop guidance for GPEA implementation, we reviewed OMB's proposed and final GPEA implementation guidance documents as well as comments on the initial draft guidance sent to OMB by federal agencies, state government organizations, and private organizations. In addition, we met with OMB officials to discuss whether OMB had received further comments from organizations on its draft implementation guidance and what actions OMB had taken in response to comments it received. We also discussed steps OMB was taking to coordinate its efforts with other agencies to which it had assigned responsibilities for developing executive-branch policies and guidance related to GPEA: the departments of Justice and Treasury, the General Services Administration (GSA), the Department of Commerce's National Institute of Standards and Technology (NIST), and the National Archives and Records Administration (NARA). We met with officials at these agencies and obtained draft GPEA implementation guidance from Justice, Treasury, and NARA. We asked OMB officials to describe their plans for tracking agencies' progress on GPEA implementation, including OMB's budget reviews and its Information Collection Budget reporting process under the Paperwork Reduction Act. In addition, we reviewed OMB's guidance to agencies on how to prepare reports describing their GPEA implementation plans and schedules.

To identify challenges or impediments that might affect GPEA implementation, we met with responsible officials at those agencies assigned executive-branch responsibilities for GPEA implementation and we reviewed pertinent documentation. In addition, we reviewed draft GPEA implementation guidance issued by NARA, Justice, Treasury, and the Federal PKI Steering Committee. We also analyzed descriptions of federal agencies' electronic information dissemination initiatives contained within reports that these agencies had sent to OMB for its Information Collection Budget report for fiscal year 2000. In addition, we analyzed our own previous reports on pertinent IT management issues.

We also reviewed studies performed by federal agencies and private industry on Internet use and electronic business; we did not independently verify information contained in these studies.

We discussed a draft of this report with officials from OMB's Office of Information and Regulatory Affairs. They offered comments of a technical or clarifying nature, which we have incorporated in the report where appropriate.

We performed our audit work from January through August 2000 in accordance with generally accepted government auditing standards.

Selected GAO Reports on Information Technology Management

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

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

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. GAO/AIMD-00-215, July 6, 2000.

Information Policy: NTIS' Financial Position Provides an Opportunity to Reassess Its Mission. GAO/GGD-00-147, June 30, 2000.

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

Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research. GAO/AIMD-00-140, June 9, 2000.

Information Technology Management: SBA Needs to Establish Policies and Procedures for Key IT Processes. GAO/AIMD-00-170, May 31, 2000.

Managing for Results: Assessing the Quality of Program Performance Data. GAO/GGD-00-140R, May 25, 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: Controls Over Software Changes at Federal Agencies. GAO/AIMD-00-151R, May 4, 2000.

Federal Information Security: Actions Needed to Address Widespread Weaknesses. GAO/T-AIMD-00-135, March 29, 2000.

Information Security: Comments on Proposed Government Information Security Act of 1999. GAO/T-AIMD-00-107, March 2, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. GAO/T-AIMD-00-72, February 1, 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.

Information Security: Weaknesses at 22 Agencies. GAO/AIMD-00-32R, November 10, 1999.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. GAO/T-AIMD-00-7, October 6, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD-00-5, October 4, 1999.

Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD-00-4, October 4, 1999.

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

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-99-280, September 15, 1999.

DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk. GAO/AIMD-99-107, August 26, 1999.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-99-227, July 30, 1999.

Information Security: Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management. GAO/T-AIMD-99-223, June 24, 1999.

Information Security: Many NASA Mission-Critical Systems Face Serious Risks. GAO/AIMD-99-47, May 20, 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.

Financial Audit: 1998 Financial Report of the United States Government. GAO/AIMD-99-130, March 31, 1999.

Customs Service Modernization: Serious Management and Technical Weaknesses Must Be Corrected. GAO/AIMD-99-41, February 26, 1999.

HUD Information Systems: Improved Management Practices Needed to Control Integration Cost and Schedule. GAO/AIMD-99-25, December 18, 1998.

IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk. GAO/AIMD-99-38, December 14, 1998.

Financial Management Service: Areas for Improvement in Computer Controls. GAO/AIMD-99-10, October 20, 1998.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-99-2, October 14, 1998.

Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-98-175, September 23, 1998.

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk. GAO/AIMD-98-92, September 23, 1998.

Social Security Administration: Technical and Performance Challenges Threaten Progress of Modernization. GAO/AIMD-98-136, June 19, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD-98-155, May 18, 1998.

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations. GAO/AIMD-98-145, May 18, 1998.

Customs Service Modernization: Architecture Must Be Complete and Enforced to Effectively Build and Maintain Systems. GAO/AIMD-98-70, May 5, 1998.

Tax Systems Modernization: Blueprint Is a Good Start But Not Yet Sufficiently Complete to Build or Acquire Systems. GAO/AIMD/GGD-98-54, February 24, 1998.

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

GAO Guides on Information Technology Management

Information Technology Investment Management: An Overview of GAO's Assessment Framework, Exposure Draft. GAO/AIMD-00-155, May 2000, Version 1.

Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Exposure Draft. GAO/AIMD-10.1.23, May 2000.

Information Security Risk Assessment: Practices of Leading Organizations. GAO/AIMD-00-33, November 1999.

Executive Guide: Information Security Management: Learning From Leading Organizations. GAO/AIMD-98-68, May 1998.

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments. GAO/AIMD-98-89, March 1998.

Business Process Reengineering Assessment Guide. GAO/AIMD-10.1.15, April 1997, Version 3.

Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making. GAO/AIMD-10.1.13, February 1997, Version 1.

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

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)**

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00