United States General Accounting Office

GAO

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

September 2000

YEAR 2000 COMPUTING CHALLENGE

Lessons Learned Can Be Applied to Other Management Challenges

GAO/AIMD-00-290

Contents

Letter 3

Appendixes

Appendix I: Timeline of Major Y2K Events 44

Appendix II: Participants in GAO's Y2K Lessons Learned Summit 52

Appendix III: GAO Reports and Testimony Statements Addressing the Year 2000 Computing Challenge 55

Appendix IV: Comments From the Office of Management and Budget 69

Abbreviations

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

GAO
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-286056

September 12, 2000

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

Dear Mr. Chairman:

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

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

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

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

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

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

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

Results in Brief

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

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

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

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

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

Background

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

Growing Concern Led to Increased Federal Y2K Response

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

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

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

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

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

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

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

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

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

The Federal Government Continues to Face Major Management Challenges

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

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

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

The Performance and Accountability Series complemented our existing High-Risk Series. Since 1990, we have periodically reported on government operations that we have identified as high risk because of their greater vulnerability to waste, fraud, abuse, or mismanagement. For example, we have designated information security and four agency IT modernization efforts (the Internal Revenue Service's tax systems modernization, FAA's Air Traffic Control Modernization, and modernization efforts at DOD and the National Weather Service) as high risk.[6]

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

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

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

Objectives, Scope, and Methodology

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

To identify lessons learned from the Y2K experience, we

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

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

(2) determine what mechanisms are needed to ensure that the critical factors behind the government's Y2K success remain in place;
- contacted the 24 major federal departments and agencies, 9 of which provided us with formal lessons learned that they had developed; and
- reviewed documents developed by other organizations, such as the President's Council on Year 2000 Conversion, the U.S. Senate Special Committee on the Year 2000 Technology Problem, and the United Nations' International Y2K Cooperation Center.[8]

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

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

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

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

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

The Congress Played a Key Oversight Role

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

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

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

[10]The Congressional Research Service's Y2K Electronic Briefing Book (*http://www.congress.gov/brbk/html/eby2k16.html*) provides a complete listing of Y2K hearings.

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

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

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

Central Leadership and Coordination of the Federal Y2K Effort Was Invaluable

Actions by the President's Council on Year 2000 Conversion, OMB, and the Chief Information Officers (CIO) Council[11] all demonstrated the value of central leadership and coordination. The President's Council focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community. The President's Council's activities fell into three areas: (1) ensuring that federal systems were ready for the date change, (2) coordinating Y2K efforts with interface partners (primarily states) for important federal services, and (3) promoting action on the Y2K problem among businesses and other governments whose failures could have had an adverse effect on the American people. To achieve its mission, the President's Council

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

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

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

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

- clarified its contingency plan instructions in early 1998 and, along with the CIO Council, adopted our Business Continuity and Contingency Guide[12] for federal use.

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

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

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

[12]GAO/AIMD-10.1.19, August 1998.

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

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

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

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

Value of Partnerships Often Cited as an Important Y2K Lesson

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

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

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

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

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

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

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

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

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

Many Methods Facilitated Communications Among Partners and Others

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

The Internet also proved to be a valuable communications channel. The Senate Special Committee on the Year 2000 Technology Problem stated in its final report[17] that use of the Internet provided an unprecedented level of organizational transparency and paved the way for effective public-private partnerships and open communications among different industries preparing for Y2K. According to the Senate report, (1) nearly every business with a presence on the World Wide Web had a link to a statement regarding Y2K compliance and (2) industry groups, associations of public managers, and trade organizations all established web sites. As a result, according to the Senate report, both companies and countries starting late on Y2K work were able to gain enormously from the shared experiences of others. An example of the effective use of the World Wide Web in providing essential Y2K compliance information was the Federal Y2K Biomedical

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

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

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

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

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

Human Capital and Budget Initiatives Were Important

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

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

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

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

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

[19] GAO/AIMD-98-85, April 30, 1998.

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

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

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

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

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

on the Year 2000 Technology Problem stated that the government cannot match private salaries and that the educational system is not providing the necessary IT skills in the quantities needed. The Office of Personnel Management has also found that salaries for information management positions in the federal government are lower than those in the private sector, and incentives available in the private sector do not exist in the federal government.

As a result of these federal human capital problems, creative solutions, such as those employed to address the Y2K problem, may need to be considered to ensure that these problems do not constrain federal IT initiatives. The CIO Council through its Federal IT Workforce Committee is working on the IT human capital issue. According to the CIO Council's fiscal year 2000 strategic plan, the committee is addressing two objectives: (1) validating and substantiating the extent of the federal IT workforce challenge and (2) developing and implementing strategies for recruitment, retention, and development of IT professionals and upgrading skills of the current workforce.

We view the government's human capital management as the missing link in the statutory and management framework that the Congress and the executive branch have established to provide for a results-oriented federal government. To help the government address this issue, we have (1) identified the range of principles that commonly underlie the human capital approaches of private sector organizations regularly cited as leaders in the area of human capital management[21] and (2) developed a human capital self-assessment checklist, which can serve as a diagnostic tool for agency leaders.[22] We intend to perform additional work in this area and plan to provide conceptual frameworks and practical tools to help agencies make substantial improvements in their human capital management policies and practices.

Funding the federal Y2K effort was also an issue. To facilitate Y2K remediation at federal agencies, in October 1998, the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999 (P.L. 105-277), was enacted. This act included $3.35 billion in contingent

[21] *Human Capital: Key Principles From Nine Private Sector Organizations* (GAO/GGD-00-28, January 31, 2000).

[22] *Human Capital: A Self-Assessment Checklist for Agency Leaders* (GAO/GGD-99-179, September 1999).

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

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

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

[23]GAO/T-AIMD-00-72, February 1, 2000.

Agency Y2K Efforts Resulted in Improved Information Technology Management

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

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

Agency Y2K Actions Benefited From High-level Management Involvement

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

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

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

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

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

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

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

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

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

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

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

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

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

Risk Analysis Allowed Agencies to Prioritize Work

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

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

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

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

[33] GAO/T-AIMD-00-72, February 1, 2000.

Improved Project Management Practices Were Implemented

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

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

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

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

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

Improved Inventories and Configuration Management

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

Improved configuration management[36] also resulted from agencies' Y2K work. Weak applications software development and change controls[37] are repeatedly highlighted in our reviews of federal agencies.[38] Without these controls, individuals can surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage. However, as a result of their Y2K efforts, agencies have reported new or strengthened configuration management practices. For example, the Department of State reported that as a result of its Y2K work, it has change control and configuration management plans that contain information about change control boards, change requests, change approval, documentation control, and version control. The

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

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

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

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

Independent Reviews Provided Valuable Management Information

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

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

Y2K Work Led to Development of Reusable Testing Practices

An effective testing program was an essential component of any Year 2000 program or project. Accordingly, as part of their Y2K activities, agencies implemented testing practices and developed test procedures that should continue to be useful. In November 1998 we issued a Y2K testing guide[40] that laid out a disciplined approach to testing activities that are hallmarks

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

[40] GAO/AIMD-10.1.21, November 1998.

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

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

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

Business Continuity and Contingency Plans Were Beneficial

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

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

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

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

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

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

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

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

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

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

[42]GAO/AIMD-98-85, April 30, 1998.

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

[44]GAO/T-AIMD-00-72, February 1, 2000.

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

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

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

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

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

Another challenge is the government's ability to address privacy concerns. It is no longer technically difficult for the government to establish databases that collect extensive personal information about large numbers of individual citizens. Individuals should be able to determine when, how, and to what extent this personal information is collected and used. However, if not properly implemented and managed, the technologies that have been developed to manage massive volumes of personal information could also be abused. For example, in May 2000 we reported[47] that the Social Security Administration had been cautious in pursuing its on-line initiatives largely because of the privacy and security concerns raised following its implementation of the on-line personal earnings and benefits estimate statement.[48]

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

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

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

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

[49] GAO/T-OCG-00-9, March 29, 2000.

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

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

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

[51] GAO/T-AIMD-00-268, July 26, 2000.

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

The Congress is considering the need for legislation to provide strong and effective central information resources and technology management leadership. In particular, although they differ in approach, three bills[53] embrace the need for a central focus point to provide effective federal government IT leadership.

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

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

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

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

[54]*Improving Government: Actions Needed to Sustain and Enhance Management Reforms* (GAO/T-OCG-94-1, January 27, 1994), *Government Reform: Using Reengineering and Technology to Improve Government Performance* (GAO/T-OCG-95-2, February 2, 1995), *Government Reform, Legislation Would Strengthen Federal Management of Information and Technology* (GAO/T-AIMD-95-205, July 25, 1995), and *Information Security: Comments on Proposed Government Information Act of 1999* (GAO/T-AIMD-00-107, March 2, 2000).

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

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

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

We believe that a federal CIO, like agency CIOs, should be primarily concerned with information resources and technology management. Indeed, as we testified in October 1997, OMB itself has raised concerns about agencies in which the CIOs had other major management responsibilities or in which it was unclear whether the CIOs' primary duty was the information resource management function.[55] Concerns such as these can only be magnified in the case of a federal CIO, whose responsibilities would be far broader than an agency CIO's.

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

Conclusions

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

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

Matter for Congressional Consideration

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

Agency Comments and Our Evaluation

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

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

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

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

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

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

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

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

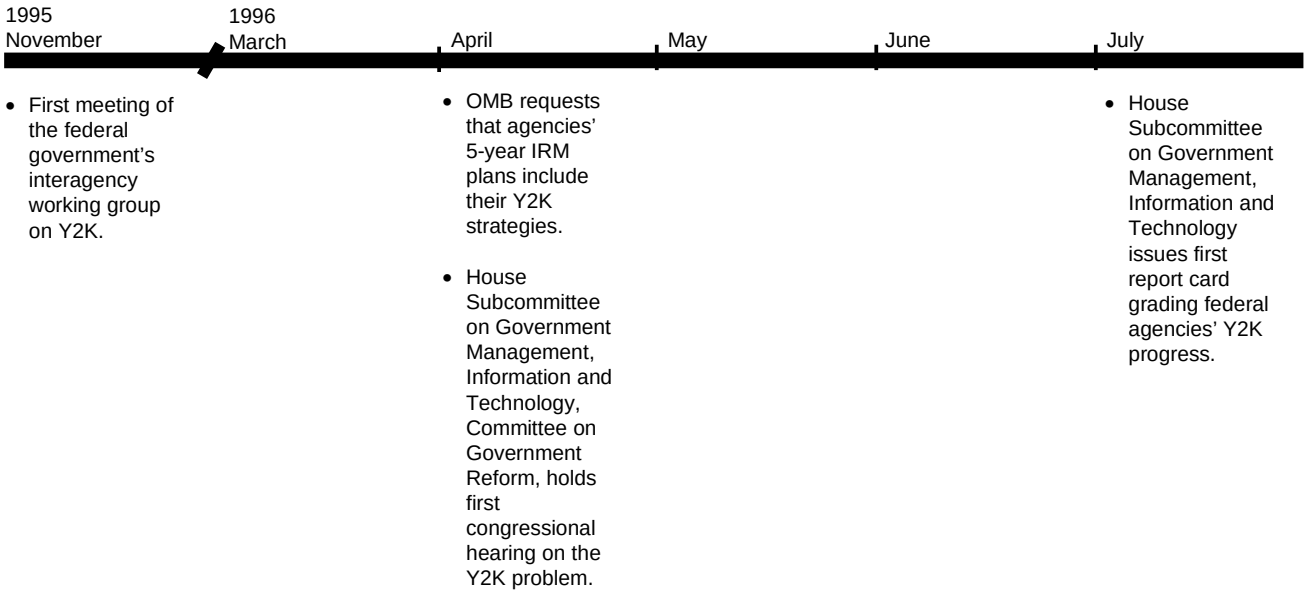
We are sending copies of this report to Senator Fred Thompson, Chairman, and Senator Joseph I. Lieberman, Ranking Minority Member, Senate Committee on Governmental Affairs; Senator Robert F. Bennett and Senator Christopher J. Dodd, former Chairman and Ranking Minority Member of the Senate Special Committee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

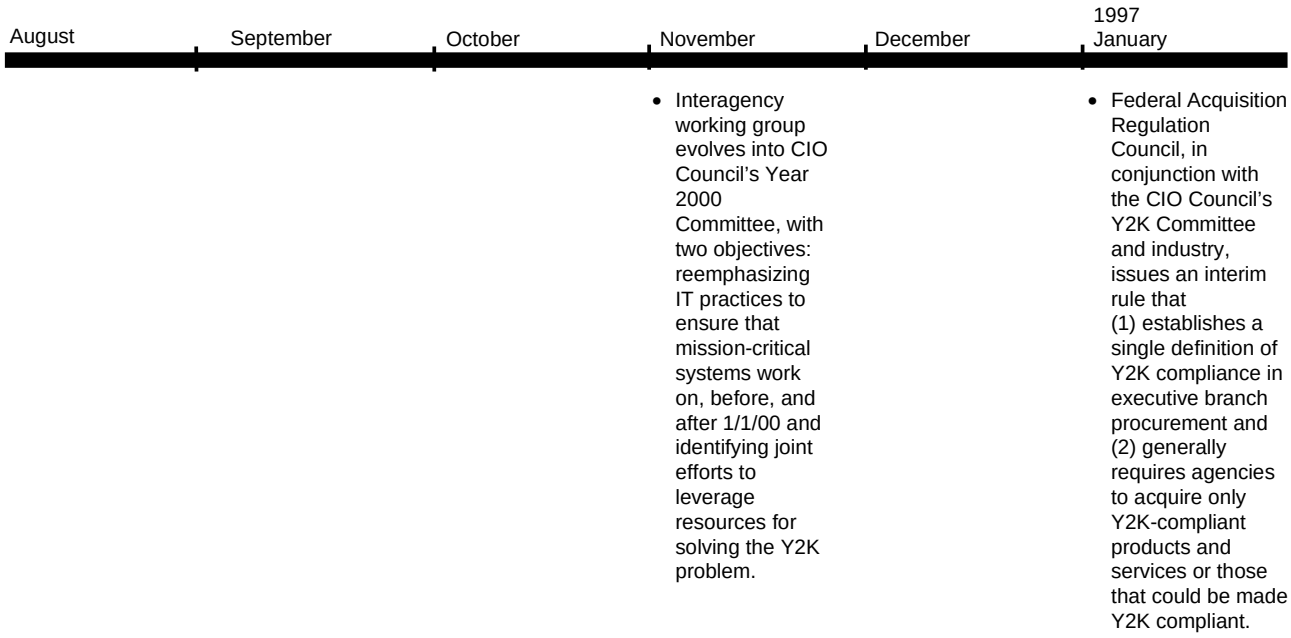
If you have any questions on matters discussed in this report, please contact me at (202) 512-6253 or by e-mail at *willemssenj.aimd@gao.gov*. Key contributors to this assignment were Linda Lambert and Glenn Spiegel.

Sincerely yours,

Joel C. Willemssen
Director, Civil Agencies Information Systems

Timeline of Major Y2K Events




August
September
October
November
December
1997
January
• Interagency working group evolves into CIO Council's Year 2000 Committee, with two objectives: reemphasizing IT practices to ensure that mission-critical systems work on, before, and after 1/1/00 and identifying joint efforts to leverage resources for solving the Y2K problem.
• Federal Acquisition Regulation Council, in conjunction with the CIO Council's Y2K Committee and industry, issues an interim rule that (1) establishes a single definition of Y2K compliance in executive branch procurement and (2) generally requires agencies to acquire only Y2K-compliant products and services or those that could be made Y2K compliant.

1997

February

- GAO designates the Y2K problem as a high-risk area for the federal government.
- OMB issues a broader Y2K strategy.

June

- OMB issues its first governmentwide progress report to the Congress; it stated that as of 5/15/97, 21 percent of 24 major departments and agencies' mission-critical systems were Y2K compliant.

July

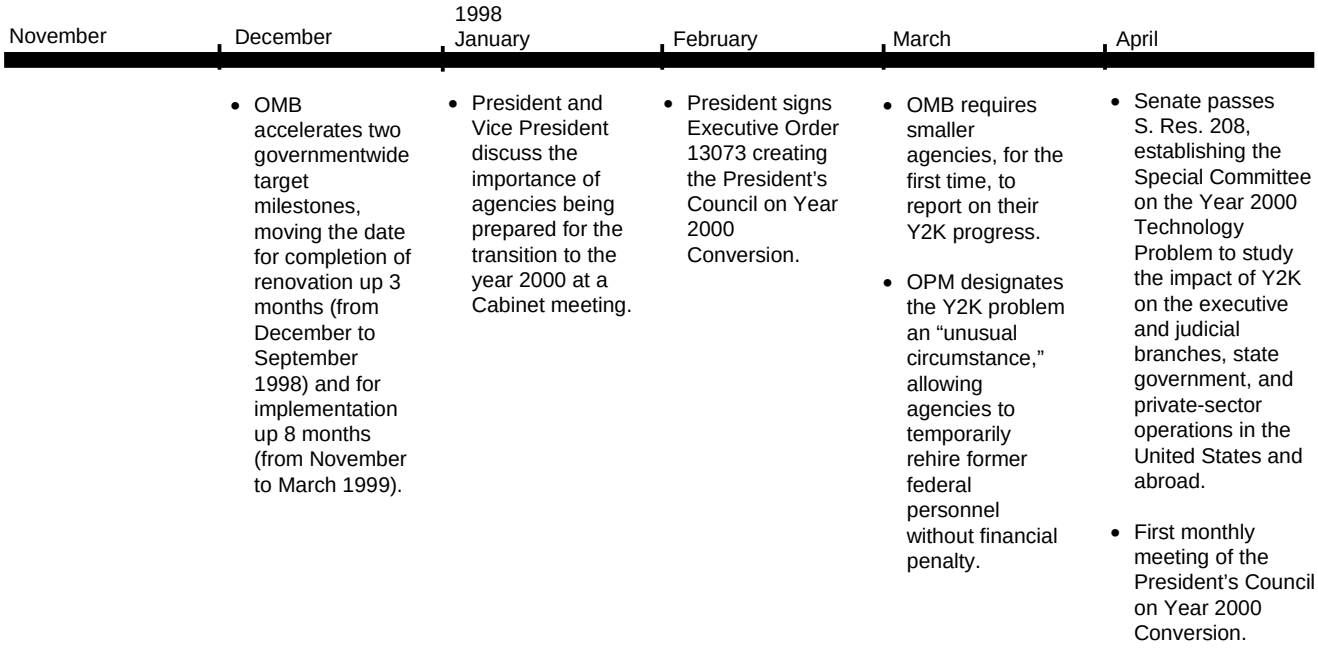
August

September

- GAO issues enterprise readiness guide: *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14).
- Recognizing that agencies were not making uniform progress, OMB's second quarterly report places them into three tiers: 4 agencies were tier 1 because they showed insufficient evidence of progress, 12 agencies were tier 2 because they showed evidence of progress but OMB had concerns, and 8 agencies were tier 3 because they appeared to be making sufficient progress.

October

- Pennsylvania hosts the first state/federal summit, sponsored by the CIO Council and the National Association of State Information Resource Executives. Participants agree on initial steps for addressing Y2K data exchange issue.


November
December
1998
January
February
March
April
• OMB accelerates two governmentwide target milestones, moving the date for completion of renovation up 3 months (from December to September 1998) and for implementation up 8 months (from November to March 1999).
• President and Vice President discuss the importance of agencies being prepared for the transition to the year 2000 at a Cabinet meeting.
• President signs Executive Order 13073 creating the President's Council on Year 2000 Conversion.
• OMB requires smaller agencies, for the first time, to report on their Y2K progress.
• OPM designates the Y2K problem an "unusual circumstance," allowing agencies to temporarily rehire former federal personnel without financial penalty.
• Senate passes S. Res. 208, establishing the Special Committee on the Year 2000 Technology Problem to study the impact of Y2K on the executive and judicial branches, state government, and private-sector operations in the United States and abroad.
• First monthly meeting of the President's Council on Year 2000 Conversion.

1998

May

- House of Representatives establishes a Year 2000 Task Force, cochaired by the Chairman of the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, and the Chairwoman of the Subcommittee on Technology, Committee on Science.
- OMB directs tier 1 and tier 2 agencies to report monthly on their Y2K progress.
- United Nations passes resolution calling on all nations to prepare critical information systems for the century date change.

June

- President's Council, in partnership with National Governors' Association, convenes first Y2K Summit with state and U.S. territory Y2K coordinators.
- Department of Justice issues a business review letter indicating that information sharing by competitors to try and solve the Y2K problem did not by itself raise an antitrust issue.

July

- GAO issues guidance: *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19).
- GAO hosts state/federal auditor conference on Y2K problem.

August

- Vice President and President's Council Chair meet with leaders of federal agencies that according to OMB, were making insufficient progress.

September

- Year 2000 Information and Readiness Disclosure Act (P.L. 105-271) enacted to promote information-sharing among companies testing their Y2K renovations.
- Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1998 (P.L. 105-277) enacted, appropriating $2.25 billion for civilian agencies and $1.1 billion for the Department of Defense for expenses related to Y2K IT conversion.
- With the help of the Small Business Administration, the Departments of Agriculture and Commerce, and other federal agencies, the President's Council sponsors the first National Y2K Action Week to help businesses, particularly small businesses, make proper Y2K assessments of important systems and take steps to prepare noncompliant systems for the century change.
- The Chair of the President's Council directs the Council's sector working groups to begin assessing their sectors.

October

November

- GAO issues guidance: *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21).

December

- President's Council helps United Nations organize first meeting of national Y2K coordinators; over 120 countries send representatives.

1999
January

- President's Council issues first quarterly assessment of the Y2K status of the nation's major sectors.
- President's Council holds its first bimonthly meeting of its Senior Advisors Group, composed of more than 20 *Fortune 500* company chief executive officers and heads of major national public-sector organizations.

February

- United Nations establishes the International Y2K Cooperation Center to promote strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on global society and the economy.

March

- President's Council, in partnership with the National Governors' Association, convenes the second Year 2000 Summit with state and U.S. territory Y2K coordinators.
- OMB's eighth quarterly report provides status of state-administered federal programs for the first time.
- OMB designates lead agencies for 42 high-impact federal programs (later updated to 43).
- With the help of the Small Business Administration, the Departments of Agriculture and Commerce, and other federal agencies, the President's Council sponsors the second National Y2K Action Week to help businesses, particularly small businesses, make proper Y2K assessments of important systems and take steps to prepare noncompliant systems for the century change.
- Federal government goal of completing Y2K implementation by March 1999 is met by 13 of the 24 major departments and agencies.

April

- President's Council issues second quarterly assessment of Y2K status of nation's major sectors.

1999

May

- OMB requires agencies to submit high-level business continuity and contingency plans.
- President's Council convenes pharmaceutical roundtable meeting.
- President's Council convenes food supply roundtable meeting.
- President's Council launches "Y2K Community Conversations" initiative to promote locally organized town hall meetings to enable citizens to hear from and ask questions of key public and private service providers.

June

- President's Council convenes hospital supply roundtable meeting.
- President signs an amendment to Executive Order 13073, creating the Information Coordination Center (ICC) to assist the Chair of the President's Council. ICC is charged with making preparations for information-sharing and coordination within the federal government and key components of the public and private sectors, coordinating agency assessments of Y2K emergencies and, if necessary, assisting federal agencies and the Council Chair in reconstitution processes.
- United Nations holds its second meeting of national Y2K coordinators; over 170 countries send representatives.

July

- President's Council convenes public safety roundtable meeting.
- Year 2000 Readiness and Responsibility Act (P.L. 106-37) enacted to establish procedures and limitations for civil actions brought for damages relating to the Y2K failure of any device or system.
- President's Council convenes Internet roundtable meeting.

August

- President's Council issues third quarterly assessment of the Y2K status of the nation's major sectors.
- President's Council convenes chemical roundtable meeting.

September

- President's Council issues *100 Days to Y2K: A Resource Guide for Small Organizations*.

October

- GAO issues guidance: *Year 2000 Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22).
- President's Council convenes education roundtable meeting.
- President's Council, in partnership with the National Governors' Association, convenes third Y2K summit with state and U.S. territory coordinators.
- OMB requires agencies to submit day one plans and revised high-level business continuity and contingency plans.

November

- President's Council issues *Y2K and You* informational booklet and personal preparedness checklist.
- President's Council issues fourth quarterly assessment of Y2K status of the nation's major sectors.
- Government earns a *B+* on final federal report card issued by the House Subcommittee on Government Management, Information and Technology.

December

- OMB announces that 99.9 percent of the federal government's mission-critical systems are Y2K compliant.
- Beginning December 30, ICC conducts 24-hour monitoring operations for the date rollover period. Staffed primarily with federal agency officials, it obtains and evaluates rollover information from a variety of sources, including federal agencies, states, localities, key private-sector organizations, foreign countries, and the media.

2000 January

- House Y2K Task Force holds final hearing on the results of the century rollover.

February

- Beginning February 28, ICC conducts monitoring operations for leap day rollover. Again staffed primarily with federal agency officials, it obtains and evaluates rollover information from a variety of sources.
- Senate Special Committee on the Year 2000 Technology Problem issues final report.

March

- GAO convenes Year 2000 Lessons Learned Summit.
- President's Council issues final report.

April

Participants in GAO's Y2K Lessons Learned Summit

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

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

David Ames
Deputy Chief Information Officer
Department of State

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

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

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

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

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

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

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

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

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

Clay Hollister
Chief Information Officer
Federal Emergency Management Agency

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

Cathy Hotka
Vice President, Information Technology
National Retail Federation

John Koskinen
Chair
President's Council on Year 2000 Conversion

Charles Madine
Senior Computer Consultant on Y2K
Federal Reserve System

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

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

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

Ed Springer
Senior Policy Analyst
Office of Management and Budget

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

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

GAO Reports and Testimony Statements Addressing the Year 2000 Computing Challenge

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

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

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

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

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

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

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

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

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

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

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

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

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

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

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

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

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

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

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

Comments From the Office of Management and Budget

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

DEPUTY DIRECTOR
FOR MANAGEMENT

September 5, 2000

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

Dear Mr. Steinhoff:

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

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

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

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

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

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

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

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

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

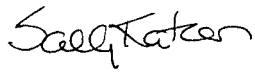
Finally, the report suggests that the Congress consider the establishment of a Federal CIO to address the other IT management challenges mentioned in the report. As the draft report notes, OMB has not supported creating a new office for this purpose. The Administration believes that, as Congress recognized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

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

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

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

Sincerely,



Sally Katzen
Deputy Director for Management

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

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

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

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

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

info@www.gao.gov

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

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

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