United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
11 a.m.
Wednesday,
June 10, 1998

YEAR 2000 COMPUTING CRISIS

Actions Must Be Taken Now to Address Slow Pace of Federal Progress

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

We are pleased to join you again today to discuss the computing crisis—of which you are well aware—posed by the upcoming change of century. No major organization, public or private, is immune from potential disruption, including a wide spectrum of government programs vital to Americans. As the world's most advanced and most dependent user of information technology, the United States possesses close to half of all computer capacity and 60 percent of Internet assets.[1] As a result, the year 2000 presents a particularly sweeping and urgent challenge for entities in this country.[2]

For this reason, in February 1997 we designated the Year 2000 problem as a high-risk area[3] for the federal government, and have published guidance[4] to help organizations successfully address the issue. Since that time, we have issued over 40 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[5] The common theme has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness, and that much more action is needed to ensure that federal agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences.

My testimony today will discuss the results of the most recent reports submitted to the Office of Management and Budget (OMB) on the slow progress made by the federal government in achieving Year 2000 compliance. In light of the pace of this progress, I will then provide our views on what needs to be done now to minimize disruptions to critical services.

[1] Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

[2] For the past several decades, automated information systems have typically represented the year using two digits rather than four in order to conserve electronic data storage space and reduce operating costs. In this format, however, 2000 is indistinguishable from 1900 because both are represented only as *00*. As a result, if not modified, computer systems or applications that use dates or perform date- or time-sensitive calculations may generate incorrect results beyond 1999.

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

[4] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997), which includes the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation), and Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, March 1998 [exposure draft]), which describes the tasks needed to ensure the continuity of agency operations.

[5] A listing of our publications is included as an attachment to this statement.

Progress in Addressing Year 2000 Continues at Slow Pace

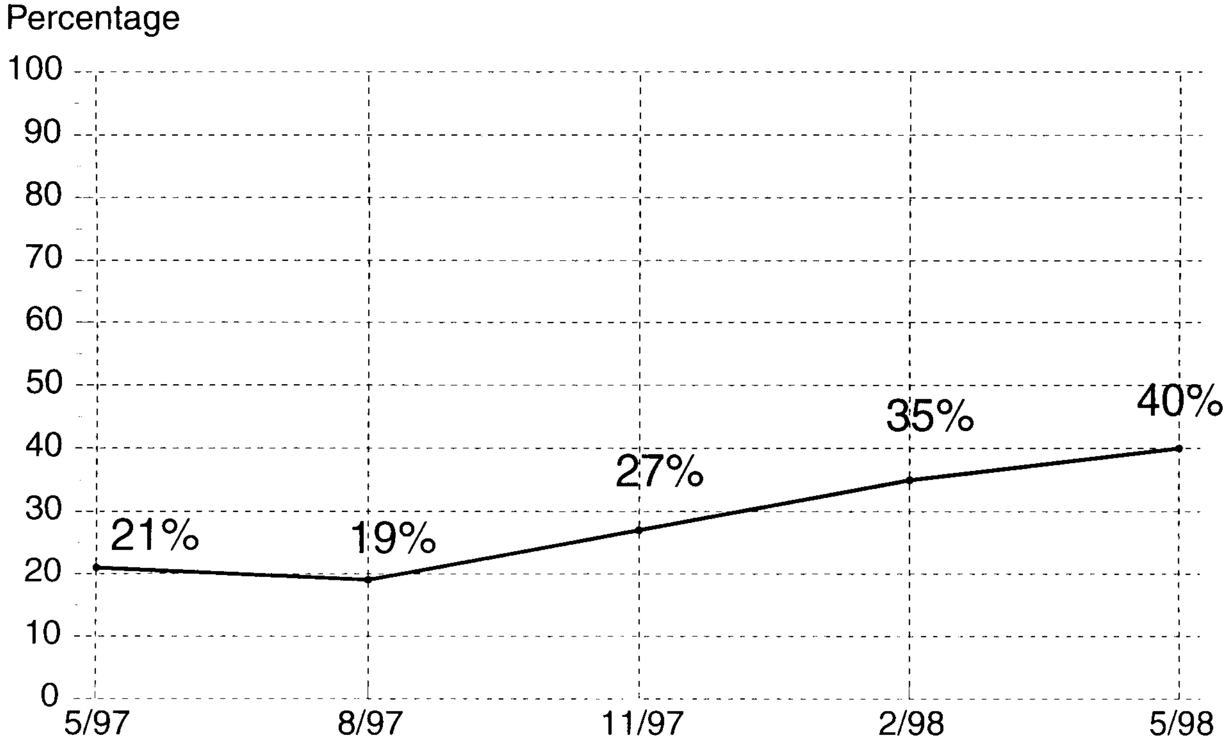
As our chart illustrates, since May 1997 OMB and the government's 24 largest departments and agencies have reported slow progress in achieving Year 2000 compliance of their mission-critical information systems.[6] In May 1997, OMB reported that about 21 percent of the government's mission-critical systems (1,598 of 7,649) were Year 2000 compliant.[7] A year later—as of last month—these departments and agencies reported a total of 2,914 systems as compliant—about 40 percent of the 7,336 mission-critical systems in their current inventories. Unless progress improves dramatically, a substantial number of mission-critical systems will not be Year 2000 compliant in time.

[6] OMB has required the following departments and agencies to report their Year 2000 readiness progress on a quarterly basis since May 1997: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, Transportation, Treasury, State, and Veterans Affairs, and the Agency for International Development, Central Intelligence Agency, Environmental Protection Agency, Federal Emergency Management Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration. The Central Intelligence Agency's reports are classified.

[7] The Social Security Administration's (SSA) mission-critical systems were not included in these totals because SSA did not report in May 1997 on a system basis. Rather, SSA reported at that time, and again in August 1997, on portions of systems that were compliant. For example, SSA reported on the status of 20,000-plus modules rather than 200-plus systems.

GAO

Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1998



A great deal of work likewise remains for agencies to meet OMB's interim target dates for renovation and validation of systems (September 1998 and January 1999, respectively). For example, according to last month's agency reports, nine have renovated less than 40 percent of their mission-critical systems due to be fixed, with two agencies having renovated less than 15 percent. This leaves little time for critical testing activities that leading organizations estimate will require at least 50 percent of total Year 2000 program time. As of last month, 16 of the 24 agencies reported that less than half of their systems requiring Year 2000 changes have completed validation.

Also of concern is that OMB, the President's Council on Year 2000 Conversion, and the Congress lack sufficient information with which to judge the progress of systems to be replaced. Agencies are not required to report on the status of specific mission-critical systems due to be replaced rather than renovated—more than 1,000 (23 percent) of the government's noncompliant mission-critical systems—unless those systems are 2 months or more behind schedule. As we have been reporting, given the federal government's poor record of delivering new systems capabilities when promised, and the immutability of the Year 2000 deadline, these replacement efforts are at high risk; it is therefore essential that reliable information that accurately reflects agencies' progress in implementing replacement systems be available. Accordingly, we previously recommended that agencies report to OMB on their progress in implementing systems intended to replace noncompliant systems.[8]

Agencies will also need a significant amount of time for essential end-to-end testing of multiple systems that have individually been deemed Year 2000 compliant. Such end-to-end testing seeks to ensure that systems collectively supporting a core business function or area operate as intended. Without such testing, systems individually deemed as compliant may not work as expected when linked together with other systems in an operational environment. These systems include not only those owned and managed by the organization, but also any external systems with which they interface. For example, the Federal Aviation Administration's Enhanced Traffic Management System monitors flight plans nationwide, controlling high-traffic situations and alerting airlines and airports to bring in more staff during times of extra traffic. Since it must exchange data with airlines' flight planning systems in order to accomplish this, end-to-end testing is essential, and would include systems for all entities involved, as well as their supporting telecommunications.

Last month's quarterly reports also disclosed other indicators that agencies and departments may not be operationally ready for the year 2000. For example:

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

- Five agencies (the Departments of Defense, Health and Human Services, Justice, Transportation, and the Treasury) reported that they had not completed assessment of their systems—almost a year behind OMB's governmentwide target of June 1997. Because these departments have taken so long to assess the readiness of their systems, it will be increasingly difficult for them to renovate and fully test all of their mission-critical systems in time.
- Only 11 of the 24 agencies reported that they had completed inventories and/or assessments of their telecommunications systems. Without compliant telecommunications systems, agencies will find it extremely difficult to carry out basic operations.
- Only six of the agencies reported that they had completed inventories and/or assessments of their embedded systems. These are special-purpose computers built into other devices; they are important because many devices built or renovated within the last 20 years use them to control, monitor, or assist in operations.

Risk of Year 2000 Disruptions Requires Leadership and Action

As a result of federal agencies' slow progress, the public faces the risk that critical services could be severely disrupted by the Year 2000 computing crisis. Financial transactions could be delayed, airline flights grounded, and national defense affected. The many interdependencies that exist among the levels of governments and within key economic sectors of our nation could cause a single failure to have wide-ranging repercussions.

The February issuance of an executive order establishing the President's Council on Year 2000 Conversion was an important step in addressing these risks. The council Chair is to oversee federal agency Year 2000 actions as well as be the spokesman in national and international forums; coordinate with state, local, and tribal governments; promote appropriate federal roles with respect to private-sector activities; and report to the President—in conjunction with OMB—on a quarterly basis.

As we testified in March,[9] the council must take strong action to avert this crisis. In a report issued in April, we detailed specific recommendations.[10] We are encouraged by action taken in response to some of our recommendations. In other areas, however, the Chair has disagreed, and some actions have not been initiated.

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

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

The current Year 2000 progress reports of most large agencies reinforce the need for the council to implement these recommendations. At this point, I would like to review the major areas in which we continue to believe that action is essential, and update the Subcommittee on what has been done.

Priority Setting

We previously testified that it was unlikely that all mission-critical systems could be made Year 2000 compliant in time.[11] We therefore recommended that the Chair of the Conversion Council establish governmentwide and agency-specific priorities for the most mission-critical business processes and supporting systems, using criteria such as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences.

In response, the Chair stated that agencies have established priorities by identifying their mission-critical systems. He further said that the council's focus at this time should be to assist agencies as they work to ensure that all of their mission-critical systems are ready for the year 2000, adding that it may be necessary at a later date for agencies to further prioritize these systems.

This approach is inconsistent with the crisis nature of the problem and does not reflect the lack of progress of the 24 agencies in correcting their mission-critical systems. The most recent set of quarterly reports reinforces our view that the time to make difficult decisions and set priorities is now, while agencies can still correct, validate, and implement essential systems. If priorities are not clearly set, the government may find that less critical systems are compliant but that some of its highest priority functions are unavailable—but could have been corrected had appropriate resources and attention been properly focused earlier.

In contrast to our country's approach, Canada has established national Year 2000 priorities. Currently, it has 44 national priorities covering areas such as national defense, food production, safety, and income security. According to Canada's Year 2000 program director, Canada wants to ensure that, at a minimum, these priority areas are fully addressed in the time remaining before 2000.

[11] GAO/T-AIMD-98-101, March 18, 1998.

End-To-End Testing

Agencies must also ensure that their mission-critical systems can reliably exchange data with other systems and that they are protected from errors that can be introduced by external systems. To achieve this goal, agencies must perform end-to-end testing for their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, work as intended in an operational environment. For example, agencies that administer key federal benefits payment programs, such as the Department of Veterans Affairs, exchange data with the Department of the Treasury, which, in turn, interfaces with various financial institutions to ensure that benefits checks are issued. In addition, Department of Defense systems interface with thousands of systems belonging to foreign military sales customers, private contractors, other federal agencies, and international organizations such as the North Atlantic Treaty Organization.

In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of the testing—and its importance—is dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange partners so that end-to-end tests can be effectively planned and executed. We therefore recommended, for the selected priorities, that lead agencies be designated to take responsibility for ensuring that end-to-end operational testing of processes and supporting systems is performed across organizational boundaries, and that independent verification and validation of such testing likewise be ensured.

In response to our recommendation, the Chair stated that agencies are currently developing such plans and obtaining independent verification and validation for their systems. He added that the council and OMB will monitor these activities and that if any difficulty arises in getting agencies to cooperate with respect to end-to-end testing, either he or OMB will intervene to resolve the matter.

Because time is short and thorough end-to-end testing of Year 2000-compliant systems and processes across organizational boundaries is essential to ensuring that services will be delivered, a more active approach is needed to ensure accountability and timely decision-making. Unless responsibility is clearly assigned, it will be difficult to ensure that all organizations participate constructively and without delay. Further, the Conversion Council will also have to assume leadership and take whatever actions are warranted should difficulties arise in obtaining needed participation and cooperation from state and local governments and the private sector.

Central Reporting Issues

OMB's reports to the Congress—based on quarterly agency progress reports—have not fully reflected the true progress of the federal government toward Year 2000 systems compliance because not all agencies have been required to report and, further, OMB's reporting requirements have been incomplete. Accordingly, we recommended (1) requiring that additional agencies that play a significant role, such as the Securities and Exchange Commission, also report quarterly to OMB, (2) requiring agencies to report on the status of their efforts to replace systems, not just on renovating those being fixed, and (3) specifying the particular steps that must be taken to complete each phase of a Year 2000 program (i.e., assessment, renovation, validation, and implementation).

OMB has acted on these recommendations. Specifically, on March 9 and April 21, 1998, OMB issued a memorandum to an additional 31 and 10 organizations, respectively, requiring that they provide information on their Year 2000 progress. The resulting reports from these organizations can further assist the Conversion Council, OMB, and the Congress in gauging progress to date, identifying risks, and raising additional issues. For example, the report submitted by the U.S. Postal Service shows that it plans to spend over $500 million on its Year 2000 effort and intends to implement its mission-critical projects by September 1998. However, the report also indicates that 21 percent of its 335 mission-critical systems are still in the assessment phase. This raises questions about whether the Postal Service's own target of this September is realistic.

In addition to requesting reports from other organizations, in its April 28, 1998, quarterly reporting guidance, OMB requested that agencies provide information on the oversight mechanism(s) used to ensure that replacement systems are on schedule. It also specified that agencies should ensure that their reporting on the completion of phases is consistent with the CIO Council's best practices guidance and our enterprise readiness guide.[12]

While we acknowledge the actions that have been taken to improve the agency reporting process, it is clear that the progress of several major departments and agencies toward ensuring Year 2000 compliance

[12] GAO/AIMD-10.1.14, September 1997.

continues to be insufficient. Accordingly, the Chair of the Conversion Council and OMB must begin requiring more frequent reporting, especially for those agencies not making sufficient progress. Such reporting would enable problems and delays to be surfaced more quickly so that necessary actions could be taken immediately. Accordingly, we now recommend that the Chair and OMB require, at an absolute minimum, monthly Year 2000 reports from those agencies not making sufficient progress.

Business Continuity and Contingency Planning

Business continuity and contingency plans should be formulated to respond to two types of failures: predictable (such as system renovations that are already far behind schedule) and unforeseen (such as a system that fails despite having been certified as Year 2000 compliant or one that, it is later found, cannot be corrected by January 1, 2000, despite appearing to be on schedule today). Therefore, agencies that develop contingency plans only for systems currently behind schedule are not addressing the need to ensure the continuity of even a minimal level of core business operability in the event of unforeseen failures. As a result, when unpredicted failures occur, agencies will be without well-defined responses and may not have enough time to develop and test effective alternatives.

Moreover, contingency plans cannot focus solely on agency systems. Federal agencies depend on data provided by business partners, as well as services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Further, those program managers responsible for core business processes should take a leading role in developing business continuity and contingency plans because they best understand their business processes and how problems can be resolved. In this manner, business continuity and contingency planning generally complements, rather than competes with, the agency's Year 2000 remediation activities. Accordingly, we recommended that the Chair require agencies to develop contingency plans for all critical core business processes.

The Chair agreed. In addition, in March 1998, OMB clarified its contingency plan instructions,[13] stating that such plans should be developed for all core business functions. Moreover, OMB and the CIO Council adopted our draft guide providing information on business continuity and contingency planning issues common to most large enterprises as a model for federal agencies.[14] Further, in its April 28, 1998, instructions, OMB asked agencies to describe their processes and activities for developing such contingency plans. Although these are positive steps, much work on contingency planning remains to be completed. In their May 1998 quarterly reports to OMB, only four agencies reported that they had drafted contingency plans for their core business processes.

Independent Verification

OMB's assessment of the current status of federal Year 2000 progress is predominantly based on agency reports—reports that have not been consistently reviewed or independently verified. Without such independent reviews, OMB and the Conversion Council have little assurance that they are receiving accurate information.

We have, in fact, found cases in which agencies' systems conversion status as reported to OMB has been inaccurate. For example, the Department of Agriculture reported 15 systems as compliant, even though they were still under development or merely planned.[15] (The department plans to delete these systems from its list of compliant systems in its next quarterly report.) In another example, the Defense Finance and Accounting Service had not performed adequate testing to assert that certain systems it had reported as compliant were capable of transitioning into the year 2000. Specifically, managers of three systems reported as compliant indicated that they had performed some tests on the transfer and storage of dates, but had not completed all necessary Year 2000 compliance testing.[16]

Agencies' May 1998 quarterly reports describe current or planned verification activities, which include internal management processes, reviews by agency inspectors general, and contracts with vendors for independent verification and validation. While this has helped provide

[13] Progress on Year 2000 Conversion, U.S. Office of Management and Budget, as of February 15, 1998.

[14] GAO/AIMD-10.1.19, March 1998 [exposure draft].

[15] See 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).

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

assurance that some verification is taking place, the full scope of verification activities required by OMB has not been articulated. Accordingly, we recommended that the Chair require agencies to develop an independent verification strategy to involve inspectors general or other independent organizations in reviewing agency Year 2000 progress.

The Chair agreed that independent assessments of agencies' Year 2000 programs and their testing and planning approaches are important, and stated that he and OMB will consider issuing more explicit directions to agencies on independent verification, especially with regard to establishing standards for the type of verification and evaluation desired. We are not aware that any such directions have yet been issued.

Workforce Issues

Obtaining and retaining adequate and skilled staff for the Year 2000 challenge has been an increasing concern. In their current quarterly reports, 10 of the 24 agencies and departments describe problems that they or their contractors have encountered in obtaining and/or retaining information technology personnel. However, no governmentwide strategy has existed to address recruiting and retaining information technology personnel with the appropriate skills for Year 2000-related work. Accordingly, we recommended that the Chair of the Conversion Council develop a personnel strategy to include (1) determining the need for various information specialists, (2) identifying needed administrative or statutory changes to waive reemployment penalties for former federal employees, and (3) identifying ways to retain key Year 2000 staff in agencies through the turn of the century.

The Chair agreed. On April 30 he stated that the Council would be working with several agencies, including the Office of Personnel Management (OPM), to examine options for ensuring an adequate number of qualified people to perform Year 2000 work. One specific action was taken on March 30, when OPM issued a memorandum stating that the Year 2000 problem was an "unusual circumstance" that would allow it to grant agencies waivers to allow them to rehire former federal personnel on a temporary basis without financial penalty. The memorandum also advised agencies of their ability to make exceptions to the biweekly limitation on premium pay when the head of an agency or designee determines that an emergency involving a direct threat to life or property exists. In addition, the Council has formed a Year 2000 workforce issues working group chaired by the Deputy Secretary of Labor. We have an ongoing review focused on assessing overall Year 2000-related personnel issues.

The Nation's Year 2000 Status

Beyond the federal government, no one knows the overall extent of our nation's vulnerability to Year 2000 risks, or the extent of our readiness. No nationwide assessment that includes the private and public sectors has been undertaken to gauge this. Accordingly, we recommended that the Council orchestrate a broad assessment of the nation's Year 2000 readiness, to include identifying and assessing the risks of the nation's key economic sectors, including risks posed by international linkages and by the failure of critical infrastructure components. Although the Chair did not directly address this recommendation in his response to our report, we are aware that the council has no plans to develop such an assessment. Without a nationwide assessment of the nation's Year 2000 status, the council will not be in a well-informed position to identify or prioritize areas of weakness and develop mechanisms to solve or mitigate those weaknesses.

Also, a coordinated, public/private effort, under the leadership of the executive branch, could provide a forum and bring together the major players in each key economic sector to effectively coordinate the nation's Year 2000 efforts and ensure that all sectors, as well as sector interdependencies, are being adequately addressed. Further, public/private forums, under the direction and oversight of the Conversion Council, could be instrumental in developing business continuity and contingency plans to safeguard the continued delivery of critical services for each key economic sector. While we do not foresee the federal government as dictating policy or requiring specific solutions, it is, however, uniquely positioned to publicize the Year 2000 computing crisis as a national priority; take a leadership role; and identify, assess, and report on the risks and necessary remediation activities associated with the nation's key economic sectors. Such plans would be all the more effective because they would bring to bear the combined and considerable influence of the federal government, state and local governments, and the private sector.

Although the Chair agreed that the Conversion Council should view the Year 2000 crisis as more than a federal systems problem and should adopt a global perspective, he disagreed with our recommendation to establish a national coordination structure using public/private partnerships in appropriate sector-based forums. He stated that the Council needs to be a catalyst, facilitator, and coordinator, but not creator and direct manager of new national forums for specific sectors of the economy.

Nevertheless, in April and May 1998, the Chair established five working groups (telecommunications, energy, financial institutions, emergency preparedness, and workforce issues) composed of federal agencies. In addition, he has identified 29 sectors headed by federal agency sector coordinators. The Chair has not provided these groups with formal, written guidance, objectives, or expectations. He has, however, told them to focus on developing a coordinated outreach plan and establish communications with public and private parties within each sector, and to monitor the Year 2000 readiness of each sector. In order for these outreach efforts to be fruitful, the working groups and coordinators will need accurate and complete information on the Year 2000 status and plans of these sectors.

It will not be enough for the Conversion Council to act as catalyst, facilitator, and coordinator. The council must also posture itself to provide Year 2000 leadership for the nation as a whole. To provide such leadership, the council must develop an approach to receiving the best guidance directly from the private sector and state and local government bodies, in addition to views and perspectives garnered by federal agency executives.

In summary, as the amount of time to the turn of the century shortens, the magnitude of what must be accomplished becomes more daunting. Greater leadership and coordination of disparate efforts is essential if government programs are to meet the needs of the public 19 months from now. The Conversion Council must play a central role in ensuring that agency action not only stays on track, but accelerates significantly.

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

GAO Reports and Testimony Addressing the Year 2000 Crisis

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).

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 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).

National Weather Service: Budget Events and Continuing Risks of Systems Modernization (GAO/T-AIMD-98-97, March 4, 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 Computers 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).

USDA Information Management: Extensive Improvements Needed in Managing Information Technology Investments (GAO/T-AIMD-97-90, May 14, 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).

(511460)

Ordering Information

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

or visit GAO’s World Wide Web Home Page at:

http://www.gao.gov

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