

GAO

Testimony

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

For Release on Delivery
Expected at
2 p.m.
Thursday,
November 4, 1999

**YEAR 2000 COMPUTING
CHALLENGE**

**Noteworthy Improvements
in Readiness But
Vulnerabilities Remain**

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



G A O

Accountability * Integrity * Reliability

Ms. Chairwoman, Mr. Chairman, and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States—with close to half of all computer capacity and 60 percent of Internet assets—is the world's most advanced and most dependent user of information technology.¹ Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.² Since that time, we have issued over 150 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.³ We have also issued guidance to help organizations successfully address the issue.⁴

The public faces the risk that critical services provided by the government and the private sector could be disrupted by the Year 2000 computing problem. As we have previously testified, financial transactions could be delayed, flights grounded, power lost, and national defense affected.⁵ Substantial progress has been made to reduce these risks and, in the fast-

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

²*High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).*

³A list of these publications is included as an appendix to this statement. These publications can be obtained through GAO's World Wide Web page at www.gao.gov/y2kr.htm.

⁴*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 Y2K Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, issued as a discussion draft in September 1999 and in final form in October 1999).*

⁵*Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998).*

paced environment of the Year 2000 issue, progress continues to be made. Today, I will discuss the federal government's progress and challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

Federal Government's Progress Noteworthy But Additional Work Remains

As the Year 2000 has grown nearer, the federal government's response to the problem has increased. Mr. Chairman, when we first testified on this problem before you in February 1997, we stated that there was much that needed to be done if the federal government was to avoid the disruption of important services, and that correcting the Year 2000 problem would be labor-intensive and time-consuming.⁶ Moreover, we testified that whether agencies succeeded and/or failed would be largely influenced by the quality of executive leadership and program management. As we reported last month, the government's Year 2000 efforts have reinforced an understanding of the importance of consistent and persistent top management attention.⁷

The Year 2000 problem has also demonstrated the importance of congressional and executive branch leadership. At the urging of congressional leaders and others, the Office of Management and Budget (OMB) and the federal agencies have dramatically increased the amount of attention and oversight given to the Year 2000 issue. Moreover, the establishment of the President's Council on Year 2000 Conversion—chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair—focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community.

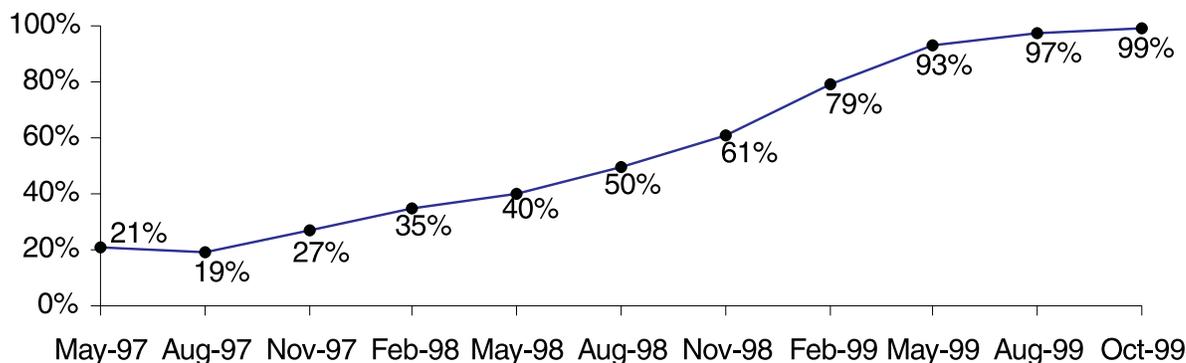
The success of these organizations' efforts is demonstrated by figure 1, which shows that the major departments and agencies have progressed from a reported compliance rate of 21 percent in May 1997 to a reported 99 percent in October 1999. While this reported governmentwide progress

⁶*Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services* (GAO/T-AIMD-97-51, February 24, 1997).

⁷*Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

is notable, the Departments of Defense, Justice, and the Treasury and the U.S. Agency for International Development still have noncompliant systems.

Figure 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-October 1999



Source: May 1997 – August 1999 data are from the OMB quarterly reports. The October 1999 data are from OMB's October 29, 1999, testimony before the House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform; and the House Subcommittee on Technology, Committee on Science.

In addition to mission-critical systems, other important areas for agencies are data exchanges, telecommunications, and building systems. Table 1 shows the reported status of the 24 major departments and agencies in these areas as of mid-August. It demonstrates that many agencies have completed work but that several others were not expected to be done until this month or next month.

Table 1: Compliance Status of Data Exchanges, Telecommunications, and Building Systems for the Major Departments and Agencies

Area	Completed	Estimated date of 1999 compliance				
		August	September	October	November	December
Data exchanges ^a	9	2	5	2	2	3
Telecommunications	8	2	9	2	2	1
Building systems ^b	7	1	7	5	2	1

^aOne agency could not forecast the completion date for its remaining exchanges.

^bThe status was not provided for one agency.

Source: Progress on Year 2000 Conversion: 10th Quarterly Report (OMB, data received August 13, 1999; report issued September 13, 1999).

While governmentwide progress has been significant, such progress has not been uniform among all federal agencies. Some agencies have long had strong Year 2000 programs in place, while others have improved their Year 2000 approaches dramatically although risks remain. Some agencies, however, require continued close attention because of the criticality of information systems to their missions and the work that remains outstanding. The following highlights representative examples of the Year 2000 progress of various agencies.

Social Security Administration (SSA): Since October 1997 we have reported on SSA's governmentwide leadership and significant progress in addressing the Year 2000 problem,⁸ and we have identified risk areas (such as the Year 2000 compliance of the systems used by the 54 state Disability Determination Services⁹ that help administer the disability programs) and made recommendations to address these risks. In July 1999, we reported that actions to implement these recommendations had either been taken or were underway.¹⁰ For example, SSA enhanced its monitoring and oversight of the state Disability Determination Services systems by establishing a

⁸*Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain* (GAO/AIMD-98-6, October 22, 1997).

⁹These include the systems in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

¹⁰*Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives* (GAO/T-AIMD-99-259, July 29, 1999).

full-time project team, designating project managers and coordinators, and requesting biweekly reports.

U.S. Customs Service: In February 1999, we testified that Customs had made good progress in addressing its Year 2000 problem, due in large part to the effective Year 2000 program management structures and processes that it had put into place.¹¹ Mr. Chairman, in a briefing last month to your Subcommittee staff on the high-impact cross-border inspection service program, we reported that Customs' progress continues. For example, Customs had developed and implemented a Year 2000 master plan and a high-impact area plan, identified and convened external business partners integral to program delivery, and reported that it had completed most planned tasks on or ahead of schedule.

Department of Veterans Affairs (VA): We have been monitoring and evaluating VA's actions to address the Year 2000 problem since 1996. During that time, we have made numerous recommendations to reduce the risk associated with Year 2000 failures. VA has been responsive to these recommendations and actions to implement them have either been taken or are underway. For example, in 1998 the Veterans Benefits Administration reassessed its mission-critical efforts for the compensation and pension on-line application and the Beneficiary Identification and Record Locator Sub-System, as well as other technology initiatives to help ensure that these critical undertakings were completed in time. As we testified last week, VA has made much progress in addressing the Year 2000 problem, although some critical tasks remain in areas such as business continuity and contingency planning.¹²

¹¹ *Year 2000 Computing Crisis: Customs is Effectively Managing Its Year 2000 Program* (GAO/T-AIMD-99-85, February 24, 1999).

¹² *Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs* (GAO/T-AIMD-00-39, October 28, 1999).

Department of Education: In September 1998, we testified that Education was very slow in implementing a comprehensive program to address Year 2000 risks.¹³ In particular, significant risks faced the department's student financial aid delivery systems, risks that involved systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. More recently, in May 1999 we testified that the Department of Education had made progress toward addressing these risks, although work remained ongoing.¹⁴ We noted that much work on renovating and validating mission-critical systems had been completed and the risk of student financial aid delivery system failures has been significantly reduced. Nevertheless, Education needed to continue making the Year 2000 problem a top priority and focus attention on such issues as end-to-end testing.

Federal Aviation Administration (FAA): In January 1998, we reported FAA had no central Year 2000 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.¹⁵ At that time, we made several recommendations, including that FAA establish plans to renovate, validate, and test all converted and replaced systems. In September 1999, we testified that FAA had addressed our recommendations and made excellent progress in its Year 2000 readiness.¹⁶ Nevertheless, FAA continued to face challenges in ensuring that its internal systems would work as intended through the year 2000 date change. For example, we found that (1) FAA had not effectively implemented its policy for managing changes to compliant systems, (2) its independent verification efforts were not adequately documented, and (3) its end-to-end testing actions were not comprehensive.

¹³ *Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems* (GAO/T-AIMD-98-302, September 17, 1998).

¹⁴ *Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains* (GAO/T-AIMD-99-180, May 12, 1999).

¹⁵ *FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically* (GAO/AIMD-98-45, January 30, 1998).

¹⁶ *Year 2000 Computing Challenge: FAA Continues to Make Important Strides, But Vulnerabilities Remain* (GAO/T-AIMD-99-285, September 9, 1999).

Internal Revenue Service (IRS): In February 1999, we testified¹⁷ that IRS had made considerable progress in completing its Year 2000 work since our testimony in May 1998.¹⁸ Nevertheless, it was behind schedule in certain critical tasks, and, in some cases such as the replacement of noncompliant personnel computers, its work is still not complete. Moreover, IRS acknowledges that its review of its information system inventory continues to identify inaccuracies—a significant risk area. Accordingly, IRS reported that, among other activities to improve the quality of its inventory, it has “wall-to-wall” inventory reviews underway at major locations, which are to be completed before the end of the calendar year. In addition, in September we reported that the two IRS business continuity and contingency plans that addressed issuing refunds and receiving paper submissions were inconsistent in two key areas—performance goals and mitigating actions.¹⁹ In testimony before you last week, IRS’ Chief Information Officer stated that the agency had addressed the suggestions in our September report.

Health Care Financing Administration (HCFA): We initially reported on HCFA’s Year 2000 program in 1997, making recommendations to improve the agency’s program management.²⁰ In subsequent reports and testimony statements, we disclosed that while HCFA had made improvements and had been responsive to our recommendations, critical Year 2000 risks and challenges remained.²¹ Most recently, we testified before your Subcommittees in September that HCFA and its contractors had made progress in addressing Medicare Year 2000 issues.²² However, as

¹⁷*IRS’ Year 2000 Efforts: Status and Remaining Challenges* (GAO/T-GGD-99-35, February 24, 1999).

¹⁸*IRS’ Year 2000 Efforts: Status and Risks* (GAO/T-GGD-98-123, May 7, 1998).

¹⁹*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).

²⁰*Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses* (GAO/AIMD-97-78, May 16, 1997).

²¹*Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy* (GAO/AIMD-98-284, September 28, 1998); *Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services* (GAO/T-AIMD-99-92, February 26, 1999); and *Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector* (GAO/T-AIMD-99-160, April 27, 1999).

²²*Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues* (GAO/T-AIMD-99-299, September 27, 1999).

stated then, until HCFA had completed its recertification tests that were then ongoing, the final status of the agency's Year 2000 compliance would remain unknown (the tests were due to be completed by November 1, 1999). Moreover, HCFA must also continue to closely monitor contractor testing with providers, which had been limited but which nevertheless had uncovered Year 2000 problems. Accordingly, given the considerable amount of work that remained, we considered it crucial that the development and testing of internal, contractor, and managed care organizations' business continuity and contingency plans move forward rapidly.

Department of Defense (DOD): Our reviews as well as those of the DOD Inspector General indicate that DOD has made noteworthy progress in its Year 2000 activities but that risks remain. For example, in March we testified that DOD had made considerable progress in the prior 3 months²³ but it faced two significant challenges: (1) completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and that key operational missions necessary for national defense can be successfully accomplished. Also, in September 1999, the DOD Inspector General reported that DOD had made significant progress in addressing some risk areas, including identifying and determining the Year 2000 readiness of its critical suppliers. Nevertheless, the Inspector General noted that DOD still faced challenges in ensuring that adequate testing is performed, testing results are sufficiently documented and analyzed, and contingency plans are viable. Moreover, as of November 1, DOD reported that it still had 31 mission-critical systems that were not Year 2000 compliant. Six of these systems are not expected to be compliant until December.

²³ *Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed* (GAO/T-AIMD-99-101, March 2, 1999).

The Government's Approach Has Improved But Risk Areas Remain

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. Accordingly, in April 1998, we made recommendations to improve the government's overall Year 2000 approach.²⁴ Since that time, the government has made progress in addressing these recommendations, although not all actions are complete.

Priority Setting: Our April 1998 report recommended that governmentwide priorities be set based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery. OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner had an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program would operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program would work. OMB directed the lead agencies to provide a schedule and milestones of key activities in their plans by April 15, and asked agencies to provide monthly progress reports.

²⁴Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

End-To-End Testing: 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, will work as intended in an operational environment. 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 testing—and its importance—are dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange partners to plan and execute effective end-to-end tests. Our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing.²⁵

Our April 1998 report recommended that, for selected government priorities, lead agencies be designated to ensure that end-to-end testing of these processes and supporting systems occurred across organizational boundaries. On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies would be pursuing during the rest of 1999 would be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, on October 18, we reported that DOD was conducting thousands of end-to-end tests in four major business functions: Health Affairs, Communications, Personnel, and Logistics.²⁶ Each of the individual test events we attended and reviewed within the four functional areas generally satisfied the key processes that our test guide defines as necessary to effectively plan, conduct, and report on end-to-end testing. We also reported in October that the Department of the Treasury's Financial Management Service, which serves as the government's financial manager, had established effective management controls in performing its portion of Year 2000 end-to-end tests for three critical business functions (Social Security payments, Supplemental Security Income payments, and Internal Revenue Service tax refund payments).²⁷

²⁵GAO/AIMD-10.1.21, November 1998.

²⁶*Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management* (GAO/AIMD-00-12, October 18, 1999).

²⁷*Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls* (GAO/AIMD-00-24, October 29, 1999).

Business Continuity and Contingency Plans: Business continuity and contingency plans are essential. Without such plans, when failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on 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. Accordingly, our April 1998 report recommended that agencies be required to develop contingency plans for all critical core business processes.

Since 1998, the federal government has improved its approach to business continuity and contingency planning. OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide for federal use. In addition, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13, OMB required agencies to submit high-level versions of these plans by June 15. In its September 1999 quarterly report, OMB required agencies to submit updated high-level business continuity and contingency plans by October 15, 1999.

As we testified before your Subcommittees last week, although more work remains, agency business continuity and contingency planning has evolved and improved since 1998.²⁸ In March 1998 we testified that several agencies reported that they planned to develop contingency plans only if they fell behind schedule in completing their Year 2000 fixes.²⁹ In June 1998, we testified that only four agencies had reported that they had drafted contingency plans for their core business functions.³⁰ By contrast, in January 1999 we testified that many agencies had reported that they had completed or were drafting business continuity and contingency plans while others were in the early stages of such planning.³¹ Also, as we testified in August, according to an OMB official, all of the major departments and agencies had submitted high-level business continuity and contingency plans in response to OMB's May 13, 1999, memorandum.³² In October, all of the major departments and agencies and the Postal Service submitted updated high-level plans to OMB.

While OMB's May 1999 memorandum directed agencies to describe their overall strategies and processes for ensuring the readiness of key programs and functions across the agency, it did not detail the format or reporting elements that agencies were to follow. Accordingly, the plans vary considerably in terms of format and level of detail. Some agencies, such as the Departments of Justice and Labor, described their general approach or strategy, while others, such as the Departments of Education and Transportation, provided program or component-entity specific plans that contained more detailed information. With respect to specific elements, all of the plans in our review³³ identified core business processes, as called for

²⁸ *Year 2000 Computing Challenge: Federal Business Continuity and Contingency Plans and Day One Strategies* (GAO/T-AIMD-00-40, October 29, 1999).

²⁹ *Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions* (GAO/T-AIMD-98-101, March 18, 1998).

³⁰ *Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress* (GAO/T-AIMD-98-205, June 10, 1998).

³¹ GAO/T-AIMD-99-50, January 20, 1999.

³² *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).

³³ While the Department of the Treasury and the General Services Administration reported that they had provided their plans to OMB, we did not receive them in time to include them in our analysis; therefore, we analyzed 23 submissions.

in our guide. In addition, we were able to identify 20 agencies that discussed their business continuity and contingency plan validation strategies in their high-level plans. These strategies encompassed a range of activities, including reviews, desktop exercises, simulations, and/or quality assurance audits.

As noted in our business continuity and contingency planning guide, a key element of such a plan is the development of a zero day or Day One risk reduction strategy. In testimony in January 1999, we noted that the Social Security Administration had developed a Day One strategy and suggested that OMB consider requiring other agencies to develop such plans.³⁴ In its September 1999 quarterly report, OMB subsequently required agencies to submit Day One strategies to it, which each of the 24 major departments and agencies and the Postal Service did. OMB subsequently asked agencies to address seven elements in their plans: (1) a schedule of activities, (2) personnel on call or on duty, (3) contractor availability, (4) communications with the workforce, (5) facilities and services to support the workforce, (6) security, and (7) communications with the public. OMB also told the agencies to consider our Day One strategy guidance carefully.

Our review of agency strategies found that about 40 percent addressed all seven elements.³⁵ For example, our testimony last week noted that the Department of Veterans Affairs addressed all of OMB's elements.³⁶ VA and its agencies had developed a Day One strategy that should help the department manage risks associated with the rollover period and better position itself to address any disruptions that may occur. The strategy included a time line of events between December 31 and January 1 and a personnel strategy and leave policy that identifies key managerial and technical personnel available to support Day One operations.

With respect to specific elements, we were able to identify 15 agencies that included a schedule of activities and 17 that addressed staffing issues. In a few cases, agencies addressed either OMB's internal communications

³⁴GAO/T-AIMD-99-50, January 20, 1999.

³⁵While the U.S. Agency for International Development and the General Services Administration reported that they had provided their plans to OMB, we did not receive them in time to include them in our analysis. Therefore, we analyzed 23 agencies' submissions.

³⁶GAO/T-AIMD-00-39, October 28, 1999.

element or external communications element but not both. Further, some elements were addressed in a general manner and/or indicated that more work needed to be completed. For example, one agency reported that it is developing procedures to ensure its ability to identify, report, and respond effectively to Year 2000-related events.

State and Local Governments Face Significant Year 2000 Risks

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts, (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised, and (3) prisoner release or parole eligibility determinations might be adversely affected.

With respect to state Year 2000 efforts, recent information from the National Association of State Information Resource Executives indicates that states have greatly improved their readiness since the beginning of this year. Table 2 provides a comparison of the percentage of mission-critical systems³⁷ reported as implemented by the states in January 1999 and in October 1999, which shows that, in general, noteworthy progress has been made during the year.³⁸

³⁷Mission-critical systems were defined as those that a state had identified as priorities for prompt remediation.

³⁸Individual states submit periodic updates to the National Association of State Information Resource Executives. For the October 28 report, about 60 percent of the states submitted their data in October; the oldest data were provided on March 11 and the most recent on October 27.

Table 2: Comparison of Percentages of Mission-Critical Systems Reported as Implemented by the States^a

Percentage implemented	Number of states on January 15, 1999 ^b	Number of states on October 28, 1999 ^c
1-24	9	0
25-49	12	1
50-74	19	3
75-99	6	39
100 percent	0	5

^aIn some cases, states did not report on their mission-critical systems, instead reporting on, for example, processes or on all systems.

^bFour states did not respond to this question.

^cTwo states did not respond to the survey.

Source: National Association of State Information Resource Executives

In addition to reporting system remediation information, as of October 28, all of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans. For nine states, however, the deadline was December 1999.

It is also essential that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Reports on local governments have highlighted Year 2000 concerns. For example:

-
- In July, we issued a letter on the reported Year 2000 status of the 21 largest U.S. cities.³⁹ On average, cities reported completing work for 45 percent of the key service areas in which they have responsibility. In addition, 2 cities reported that they had completed their Year 2000 efforts, 9 expected to complete Year 2000 preparations by September 30, 1999, and the remaining 10 cities expected to complete their preparation by December 31.⁴⁰ In addition, 7 cities reported completing Year 2000 contingency plans, while 14 reported that their plans were still being developed.
 - Also in July, the National League of Cities reported on its survey of 403 cities conducted in April 1999. This survey found that (1) 92 percent of cities had a citywide Year 2000 plan, (2) 74 percent had completed their assessment of critical systems, and (3) 66 percent had prepared contingency plans. (Of those that had not completed such plans, about half stated that they were planning to develop one.) In addition, 92 percent of the cities reported that they expected that all of their critical systems would be compliant by January 1, 2000; 5 percent expected to have completed between 91 and 99 percent, and 3 percent expected to have completed between 81 and 90 percent of their critical systems by January 1.
 - In June, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed systems testing. In addition, 190 counties had prepared contingency plans while 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan from April through June, 64 from July through September, 18 from October through December, and 10 did not yet know.

Of critical importance to the nation are services, such as law enforcement, that are essential to the safety and well-being of individuals across the country. For the most part, responsibility for ensuring the continuity of law enforcement operations resides with thousands of state and local

³⁹ *Reported Y2K Status of the 21 Largest U.S. Cities* (GAO/AIMD-99-246R, July 15, 1999).

⁴⁰ In most cities, the majority of city services were scheduled to be completed before this completion date. For example, Los Angeles planned to have all key city systems ready by September 30, except for its wastewater treatment systems, which were expected to be completed in November.

jurisdictions. One critical system—the National Crime Information Center 2000—is operated by the Federal Bureau of Investigation and provides law-enforcement users in 80,000 U.S. and foreign agencies critical access to information on criminal activities. Mr. Chairman, we recently briefed your Subcommittee staff on the status of this system. While the Federal Bureau of Investigation reported that its Year 2000 remediation, validation, and implementation activities were completed for the National Crime Information Center 2000, the readiness of five state-level partners was uncertain. Specifically, in assessing the readiness of each state, Puerto Rico, and the District of Columbia, the Bureau found that 47 were Year 2000 ready, but that five had not completed Year 2000 remediation at the time of the assessment. The Bureau plans to continue reviewing the readiness status of these five.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council on Year 2000 Conversion developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly, multistate conference calls with state Year 2000 coordinators.
- In July 1998, March 1999, and October 1999 the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.⁴¹ In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.⁴² Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant.

Table 3 summarizes the latest information on state-administered federal human services programs reported by OMB on September 13, 1999.⁴³ The table indicates that while many states⁴⁴ reported their programs to be compliant, a number did not plan to complete Year 2000 efforts until the last quarter of 1999. For example, nine states did not expect to be compliant until the last quarter of 1999 for Child Support Enforcement, seven states for Food Stamps, and four states for Unemployment Insurance. Moreover, Year 2000 readiness information was unknown in many cases. For example, according to OMB, the status of 16 states' Low

⁴¹ *Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs* (GAO/AIMD-99-28, November 6, 1998).

⁴² *Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs* (GAO/T-AIMD-99-91, February 24, 1999).

⁴³ For Medicaid, OMB reports on the two primary systems that states use to administer the program: (1) the Integrated Eligibility System, used to determine whether an individual applying for Medicaid meets the eligibility criteria for participation and (2) the Medicaid management information system (MMIS), used to process claims and deliver payments for services rendered. Integrated eligibility systems are also often used to determine eligibility for other public assistance programs, such as Food Stamps.

⁴⁴ In the context of this testimony, the term states can include the District of Columbia and U.S. territories, such as Puerto Rico.

Income Home Energy Assistance programs was unknown because applicable readiness information was not available.

Table 3: Reported State-level Readiness for Federally Supported Programs^a

Program	Compliant ^b	Estimated compliance date before August 1999 ^c	Expected date of 1999 compliance							Unk. ^d	N/A ^e
			Aug.	Sept.	Oct.	Nov.	Dec.				
Child Nutrition	41	1	4	4	2	0	2	0	0		
Food Stamps	39	0	3	5	3	4	0	0	0		
Women, Infants, and Children	45	0	0	2	3	3	1	0	0		
Child Care	25	12	0	2	2	3	0	6	4		
Child Support Enforcement	23	9	2	7	4	3	2	4	0		
Child Welfare	23	14	1	3	5	3	0	5	0		
Low Income Home Energy Assistance Program	25	2	3	3	2	0	0	16	3		
Medicaid – Integrated Eligibility System	25	18	0	5	4	0	0	2	0		
Medicaid – Management Information System	22	16	5	4	4	1	0	2	0		
Temporary Assistance for Needy Families	27	15	2	4	2	1	0	3	0		
Unemployment Insurance	39	0	0	10	3	0	1	0	1		

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bOMB defined compliant as when the state or territory had determined that its systems were able to provide services, whether directly or indirectly, to beneficiaries.

^cIn many cases, the report indicated a date instead of whether the state was compliant. According to OMB, in some cases, while the estimated dates had passed, confirmation of completion had not been received from the federal agencies.

^dUnknown indicates that, according to OMB, no information was reported by the agency.

^eN/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 10th Quarterly Report (OMB, data received August 13, 1999; report issued September 13, 1999).

The information in the OMB report was gathered, but not verified, by the Departments of Agriculture, HHS, and Labor, based on submissions by the states and territories. As a result, some of the state information reported by

OMB may not be accurate or up-to-date. For example, in five cases, state programs cited as compliant by OMB in its June quarterly report had estimated compliance dates of October 1999 or later in its September quarterly report.

Further, as we testified last month, the late reported compliance dates of some states are problematic since schedule delays or unexpected problems could well arise.⁴⁵ Indeed, reported schedule delays have now occurred in 8 of the 10 state-administered programs since OMB's June 1999 report.⁴⁶ For example, OMB's June report showed that three states had estimated compliance dates in the last quarter of 1999 for Food Stamps, while the most recent OMB report indicates that seven states now have estimated fourth quarter compliance dates. To illustrate, the June OMB report indicated that a state and a territory were due to be compliant in June for Food Stamps, but the September OMB report indicated that the date for these entities had moved to November 1999.

In addition to obtaining state-reported readiness information, the three federal departments are taking other actions to assess the ability of state-administered programs to continue operating successfully into the next century.

Department of Agriculture: Agriculture's Food and Nutrition Service (FNS) is responsible for three state-administered federal human services programs—Child Nutrition; Food Stamps; and Women, Infants, and Children. To obtain assurance that state systems are compliant, FNS' regional offices are collecting readiness status information from states as part of their monitoring. Moreover, in June 1999, FNS required its regions to provide, for each program, a copy of either a state letter certifying that it was Year 2000 compliant or a business continuity and contingency plan. As of August 25, 1999, FNS had received

- 15 certifications and 6 business continuity and contingency plans for Child Nutrition;
- 22 certifications and 16 business continuity and contingency plans for Food Stamps; and

⁴⁵Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs (GAO/T-AIMD-00-9, October 6, 1999).

⁴⁶There was no change in one state-administered federal program, and the number of states with estimated compliance dates in the last quarter declined by one for a second program.

-
- 25 certifications and 21 business continuity and contingency plans for Women, Infants, and Children.

Although agency officials instructed FNS regional offices to require state agencies for all three programs to prepare business continuity and contingency plans, it remains unclear whether all states have adequate plans to ensure the continuity of these programs. For example, a June 18 FNS document summarizing the agency's review of contingency plans received to date noted that "all need work." As of September 15, FNS officials told us that only two states had submitted suitable contingency plans. FNS intends to have its contractor review contingency plans for those states that reported that they expected to be compliant after September 30, 1999.

Department of Health and Human Services: Six of the 10 state-administered federal human services programs are overseen by either one of two HHS component entities, HCFA or the Administration for Children and Families (ACF). As we stated in October, HCFA has adopted an approach that includes three rounds of on-site contractor reviews of states (performed in conjunction with HCFA regional and headquarters offices) using a standard methodology.⁴⁷ With respect to the risk levels assigned to the states, as of October 4, 1999,

- 4 eligibility systems and 5 MMISs were assessed at high risk,
- 13 eligibility systems and 8 MMISs were assessed at medium risk, and
- 36 eligibility systems and 40 MMISs were assessed at low risk.⁴⁸

HCFA's current state risk ratings represent an overall improvement from those assigned after the first round of reviews, although many issues continue to be unresolved with the states.

⁴⁷Reported Medicaid Year 2000 Readiness (GAO/AIMD-00-22R, October 5, 1999).

⁴⁸Forty state risk ratings were based on second-round visits (conducted between May and September 1999), while 13 state risk ratings in the low category are based on the results of first-round visits because the states were not visited in the second round.

To complement its system reviews, HCFA obtained another contractor to review state business continuity and contingency plans. In June 1999, HCFA's business continuity and contingency plan contractor began reviewing the quality of state plans through either a desk audit alone or both a desk audit and an on-site visit. Of the 33 states and two territories that have been reviewed by the contractor as of October 1, 1999,⁴⁹ 11 were high risk, 11 were medium risk, and 13 were low risk.

Regarding the other five HHS state-administered federal programs, ACF modeled its state assessment program after that of HCFA. Table 4 shows the number of states placed in each risk assessment level as of October 21.

Table 4: Summary of Risk Levels as of October 21, 1999

Program	Number of state reports	Risk levels		
		High	Medium	Low
ACF - Child Care	55	3	16	36
ACF - Child Support Enforcement ^a	54	3	12	39
ACF - Child Welfare	54	0	14	40
ACF - Low Income Home Energy Assistance Program ^a	54	1	16	37
ACF - Temporary Assistance for Needy Families ^a	54	3	9	42

^aThese programs were not evaluated for one of the U.S. territories or a territory does not have the program.

According to an ACF official, although the agency has not completed a reassessment of state risk ratings, most state programs with high or medium risk ratings have improved their status since the original assessment was completed (May through September).

Department of Labor: With respect to Unemployment Insurance, the 53 State Employment Security Agencies (SESAs) use their own systems to pay unemployment insurance compensation benefits to eligible workers and collect state unemployment taxes from employers. As of November 1,

⁴⁹As of October 1, 1999, 16 state business continuity and contingency plans had not been reviewed, and 2 states had not provided their plans to HCFA.

according to the Labor Department, 51 of 53 SESAs reported that their benefits systems were Year 2000 compliant, while 50 of the 53 tax systems were reported as such.

In September 1998, Labor established a valuable tool in gauging the readiness of state Unemployment Insurance systems by requiring that all SESAs arrange for independent verification and validation. Based on the results of these reviews, Labor has indicated that the Secretary will be sending letters to the governors of 11 states considered to be in need of further attention concerning their Year 2000 compliance efforts. Labor reported to us that it would continue to work aggressively with the SESAs needing further attention.

To provide further assurance that unemployment insurance benefits will continue without interruption in the Year 2000, Labor has required that the SESAs develop detailed business continuity and contingency plans for their automated systems. According to Labor, a PC-based Automated Contingency System has been developed to permit the interim payment of benefits should a Year 2000 failure occur. Labor reports that nine states have adopted this system as part of their contingency planning.

Mixed Year 2000 Progress in Key Sectors

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the President's Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.⁵⁰ The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council has formed a senior advisors group of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on crosscutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures.

Our April 1998 report also recommended that the President's Council develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic

⁵⁰GAO/AIMD-98-85, April 30, 1998.

sectors—including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Council then began issuing quarterly public reports summarizing these assessments, beginning in January 1999.

The Council's August 1999 report stated that important national systems will make a successful transition to the year 2000 but that much work, such as contingency planning, remains to be done.⁵¹ In particular, the Council expressed a high degree of confidence in five major domestic areas: financial institutions, electric power, telecommunications, air travel, and the federal government. For example, the Council stated that on August 2, federal bank, thrift, and credit union regulators reported that 99 percent of federally insured financial institutions have completed testing of critical systems for Year 2000 readiness.

The Council had concerns in four significant areas: local government, health care, education, and small businesses. For example, according to the Council report, many school districts could move into the new century with dysfunctional information technology systems, since only 28 percent and 30 percent, respectively, of Superintendent/Local Educational Agencies and postsecondary institutions reported that their mission-critical systems were Year 2000 compliant.

In the international arena, the Council stated that the Year 2000 readiness of other countries was improving but remains a concern. The Council reported that the June 1999 meeting of National Year 2000 Coordinators held at the United Nations found that the 173 countries in attendance were clearly focused on the Year 2000 problem but that many will likely not have enough time or resources to finish preparations before the end of 1999.

In addition to our work related to federal, state, and local government Year 2000 progress, we have also issued several publications related to key economic sectors. Our analysis has identified sectors that are leaders in resolving Year 2000 problems, others that require sustained attention

⁵¹The Council's three reports are available on its web site, www.y2k.gov. The Council's next report is due to be released shortly.

because of their importance and continued risk, and a few that are lagging behind. In addition, variance in the level of readiness within segments of a sector can exist. The following are representative samples of the readiness of key sectors.

Banking and Finance Sector: The banking and finance sector is considered a Year 2000 leader. A large portion of the institutions that make up this sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies⁵² to ensure that the institutions they oversee are ready to handle the Year 2000 problem.⁵³ Regulators had made significant progress in assessing the readiness of member institutions and in raising awareness on important issues, such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 activities found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, regulators faced the challenge of ensuring that they were ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

⁵²The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.

⁵³*Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain* (GAO/T-AIMD-98-305, September 17, 1998).

In April, we reported that the Federal Reserve System—which is instrumental to our nation’s economic well-being since it provides depository institutions and government agencies with services such as processing checks and transferring funds and securities—had effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.⁵⁴ It also was effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it was fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported⁵⁵ that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but that they planned to complete their actions by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that their systems were ready for the date change and that they had begun testing with the financial organizations that depend on these systems. We further found that seven large U.S. banks and securities firms that we visited were taking actions to address their international risks. Finally, U.S. banking and securities regulators were addressing the international Year 2000 risks of the institutions that they oversee.

⁵⁴ *Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion* (GAO/AIMD-99-78, April 9, 1999).

⁵⁵ *Year 2000: Financial Institution and Regulatory Efforts to Address International Risks* (GAO/GGD-99-62, April 27, 1999).

With respect to the insurance industry, in March, we concluded that the insurance regulator presence in the Year 2000 area was not as strong as that exhibited by the banking and securities industry.⁵⁶ State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared with other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report, in April⁵⁷ we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Telecommunications: In September, we reported that basic network services are unlikely to be immediately disrupted by Year 2000-related problems if networks are left unremediated, according to experts who have been tracking and studying the telecommunications industry's Year 2000 risks.⁵⁸ However, telecommunications carriers could still experience problems with network maintenance, service billing, or operator interfaces, such as incorrect date or day-of-week displays. We also said that major U.S. public telecommunications carriers reported making good progress in remediating their networks and supporting systems in order to

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

⁵⁷*Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness* (GAO/GGD-99-87, April 30, 1999).

⁵⁸*Year 2000 Computing Crisis: Readiness of the Telecommunications Industry* (GAO/AIMD-99-293, September 30, 1999).

prevent these types of Year 2000-related problems. Less information was available on the status of medium and small carriers but efforts to collect more data on these carriers were ongoing.

From an international telecommunications perspective, in July 1999, the Network Reliability and Interoperability Council reported that while countries around the globe continue to make progress, their efforts—with some exceptions—have not matched the pace of efforts in the United States and Canada. Regions considered to be at high risk were Central and South America (including Mexico), the Indian sub-continent, Sub-Sahara Africa, Eastern Europe, the Middle East and North Africa (excluding Israel), and Asia Pacific. The Network Reliability and Interoperability Council cautioned, however, that the information available was limited and varied in its view from source to source. Moreover, the results of the assessment varied widely within each region. For example, while Asia Pacific is considered to be a region of high risk, some nations within that region, such as Australia, are considered to be at low risk.

Energy Sector: As we testified last week, while progress had been made in making the nation's nuclear power plants and fuel processing facilities Year 2000 ready, some risk remained.⁵⁹ At particular risk were the two plants that do not yet have their nonsafety systems ready, especially the one with a completion date scheduled for more than 30 days from now. Similarly, the four nuclear fuel facilities that were not Year 2000 ready by September 1, 1999, raise concern. Likewise, not knowing the current Year 2000 status of all 14 decommissioned plants with spent fuel also raised concern. Finally, the lack of information on two key issues—independent reviews of Year 2000 testing and emergency Year 2000 exercises—and the lack of requirements for Day One planning increases the Year 2000 risk to the nuclear power industry.

To further reduce risks, we pointed out that the Nuclear Regulatory Commission (NRC) and the nuclear power industry could still take specific actions to ensure Year 2000-related plant safety.

- First, NRC should evaluate and report on the Year 2000 status of all decommissioned plants with spent fuel status that previously reported that they were not Year 2000 ready.

⁵⁹ *Y2K Computing Challenge: Nuclear Power Industry Reported Nearly Ready; More Risk Reduction Measures Can Be Taken* (GAO/T-AIMD-00-27, October 26, 1999).

-
- Second, NRC should survey the 103 operational nuclear power plants to gain an understanding of what independent reviews were completed. Based on this information, NRC should then identify plants that may need additional reviews.
 - Third, NRC should obtain information on the scope and extent of nuclear power plants' emergency exercises, and whether these exercises have incorporated Year 2000 scenarios.
 - Finally, NRC should ensure that all nuclear facilities have developed Day One plans.

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.⁶⁰ We therefore suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness, and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power.

Subsequent to our report, on August 3, 1999, the North American Electric Reliability Council released its fourth status report on electric power systems. This report disclosed those organizations that were Year 2000 ready or Year 2000 ready with limited exceptions. According to the Council, as of June 30, 1999, 251 of 268 (94 percent) of bulk electric organizations were Year 2000 ready or Year 2000 ready with limited exceptions.⁶¹ In addition, this report stated that 96 percent of local distribution systems were reported Year 2000 ready.⁶² The North American Electric Reliability

⁶⁰ *Year 2000 Computing Crisis: Readiness of the Electric Power Industry* (GAO/AIMD-99-114, April 6, 1999).

⁶¹ The North American Electric Reliability Council reported that 64 of these organizations had exceptions but that it "believes that the work schedule provided to complete these exception items in the next few months represents a prudent use of resources and does not increase risks associated with reliable electric service into the Year 2000."

⁶² This was based on the percentage of the total megawatts of the systems reported as Year 2000 ready by investor-owned, public power, and cooperative organizations. The report did not identify the number of local distribution organizations that reported that they were Year 2000 ready.

Council stated that the information it uses is principally self-reported but that 84 percent of the organizations reported that their Year 2000 programs had also been audited by internal and/or external auditors.

In May we reported⁶³ that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. For example, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions to the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures, and (2) develop national-level contingency plans.

The results of the latest oil and gas industry survey were provided at the October 21 Federal Energy Regulatory Commission Technical Conference. This survey found that 92 percent of oil and gas companies' business systems, 93 percent of their embedded systems, and 83 percent of their supply chain were Year 2000 ready. In addition, the survey found that 90 percent of the oil and gas companies had contingency plans in place, and 77 percent had tested them.

Transportation Sector: Airports make up a key component of the nation's transportation sector. In January we reported on our survey of 413 airports, finding that while the nation's airports were making progress in preparing for the year 2000, such progress varied.⁶⁴ Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date. Moreover, about half of the airports in our survey did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready

⁶³ *Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries* (GAO/AIMD-99-162, May 19, 1999).

⁶⁴ *Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem* (GAO/RCED/AIMD-99-57, January 29, 1999).

by June 30 were small airports, 26 of them were among the nation's largest 50 airports.

More recently, we testified in September on the Year 2000 information collected by the Federal Aviation Administration on 113 U.S. airports.⁶⁵ According to FAA's information at that time, about 20 percent of the 113 airports reported that they had completed their Year 2000 preparations. Another 58 percent estimated that they would complete Year 2000 efforts by September 30, and the remaining 22 percent either planned on a later date or did not provide an estimated completion date. Among the group planning to complete their Year 2000 efforts after September 30 but by November 30 were five of the nation's largest international airports.

Just 2 days ago, the Department of Transportation announced that none of the 565 airports regulated by FAA had been found to have Year 2000 problems that will affect their ability to meet regulatory safety requirements—which would include airfield operations such as aircraft rescue and firefighting response but not ground transportation systems. To make this assessment, FAA determined whether airport operators had taken the necessary measures to ensure that such systems were Year 2000 compliant or had developed an alternate means for complying with these requirements. For example, in the case of runway and taxiway lighting, FAA required that an airport operator ensure that computers used to control these lights were Year 2000 compliant or that control of the lights could be performed manually.

Another essential element in this sector is the readiness of airlines. According to FAA's information at the time of our September testimony, about 33 percent of 146 airlines reported that their systems were Year 2000 compliant. Another 35 percent planned to complete their Year 2000 efforts by September 30, and the remaining 32 percent either planned on a later date or did not provide any date. Among the group planning to complete their Year 2000 work after September 30 but by December 31, 1999 were four of the nation's major airlines.

⁶⁵GAO/T-AIMD-99-285, September 9, 1999.

Education: On September 21, we reported on the Year 2000 readiness status of 25 large school districts, showing that much work remained.⁶⁶ Of the 25 school districts surveyed, seven reported that all of their systems that support mission-critical business functions were Year 2000 compliant. Two districts reported that their mission-critical systems would be Year 2000 compliant by the end of September. The remaining 16 districts reported that their systems would be ready by the last quarter of 1999 or later, including nine reporting that compliance would be achieved after November 30, 1999.

More recently, Education completed surveys of a random sample of 1,200 school districts and 1,600 postsecondary institutions during the first week of October. Regarding the 985 school district respondents, (1) 64 percent reported that all mission-critical systems were compliant, (2) 96 percent expected that all of their mission-critical systems would be compliant by January 1, 2000, (3) 65 percent reported that contingency plans were completed, and (4) 83 percent expected that contingency plans would be completed by January 1. For the 1,352 postsecondary institution respondents, (1) 61 percent reported that all mission-critical systems were compliant, (2) 97 percent expected that all of their mission-critical systems would be compliant by January 1, 2000, (3) 73 percent reported that contingency plans were completed, and (4) 88 percent expected that contingency plans would be completed by January 1.

Health Care Sector: This sector, which includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment, is not as far along in its readiness as other sectors. In July we reported⁶⁷ that HCFA had taken aggressive and comprehensive outreach action with regard to its over 1.1 million health care providers that administer services for Medicare-insured patients.⁶⁸ Despite these efforts, HCFA data showed that provider participation in its outreach activities had been low. Our July report also found that although many surveys had been completed in 1999 on the Year

⁶⁶*Reported Year 2000 (Y2K) Readiness Status of 25 Large School Districts* (GAO/AIMD-99-296R, September 21, 1999).

⁶⁷*Year 2000 Computer Crisis: Status of Medicare Providers Unknown* (GAO/AIMD-99-243, July 28, 1999).

⁶⁸Examples of such providers are hospitals, laboratories, physicians, and skilled nursing/long-term care facilities.

2000 readiness of health care providers, none of the 11 surveys we reviewed provided sufficient information with which to assess the Year 2000 status of the health care provider community. Each of the surveys had low response rates, and several did not address critical questions about testing and contingency planning.

To reduce the risk of Year 2000-related failures in the Medicare provider community, our July report suggested that HCFA consider, for example, using additional outreach methods, such as public service announcements, and set milestones for Medicare contractors for testing with providers. We also made suggestions to the President's Council on Year 2000 Conversion's healthcare sector working group, including a suggestion to consider working with associations to publicize those providers who respond to future surveys in order to increase survey response rates.

Of Medicare's 39 million beneficiaries, about 6.9 million are enrolled in 383 managed care organizations. We testified in September that HCFA, with assistance from a contractor, performed a risk assessment of 425 managed care organizations⁶⁹ using certification statements and associated qualifications and other criteria.⁷⁰ HCFA's June 1999 risk assessment concluded that 94 managed care organizations were high risk (22 percent), 314 were medium risk (74 percent), and 17 were low risk (4 percent). Also, as of September 2, 1999, HCFA had received business continuity and contingency plans from 310 of the 383 managed care organizations. Its review of these 310 plans concluded that 69 percent needed major improvement, 18 percent needed minor improvement, and 13 percent were reasonable.

⁶⁹Since July 1999, the number of managed care organizations decreased from 425 to 383, because 52 left the Medicare program while 10 new managed care organizations joined.

⁷⁰GAO/T-AIMD-99-299, September 27, 1999.

With respect to biomedical equipment, on June 10 we testified⁷¹ that, in response to our September 1998 recommendation,⁷² HHS, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As we recently testified, as of October 4, 1999, 4,288 biomedical equipment manufacturers had submitted data to the clearinghouse.⁷³ About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (342 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, a component agency of HHS, the 342 manufacturers reported 1,035 specific products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 429 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and testified in October that we found a total of 32,598 products.⁷⁴ Of these products, 17,505 were reported as not employing a date, 9,585 were reported as compliant, 4,053 were shown as not compliant, and the compliance status of 1,455 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report⁷⁵ also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999 as well the Food and Drug Administration announced that it planned to develop a list of critical care/life support

⁷¹*Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment* (GAO/T-AIMD-99-209, June 10, 1999).

⁷²*Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown* (GAO/AIMD-98-240, September 18, 1998).

⁷³*Year 2000 Computing Challenge: Compliance Status Information on Biomedical Equipment* (GAO/T-AIMD-00-26, October 21, 1999).

⁷⁴Because of limitations in many of the manufacturers' web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 32,598 products that we counted.

⁷⁵GAO/AIMD-98-240, September 18, 1998.

medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed.

The Food and Drug Administration identified 90 types of products that it refers to as computer-controlled, potentially high-risk devices, and identified 803 manufacturing sites that produce equipment sold in the United States. Of these sites, a Food and Drug Administration contractor completed 80 site visits and had prepared 62 assessment reports. We reviewed 25 manufacturer site visit reports that were completed by the examiners and available to us as of September 10, 1999. For 20 of these assessments, the examiners' assessed concern was low. At the 5 remaining manufacturers' sites, the examiner found at least one item of moderate concern, such as test planning and procedures. According to the survey project manager, the areas identified in the site visit reports as medium risk do not constitute a risk to patient health or safety.

In testimony on October 28,⁷⁶ we also reported on the results of a Department of Veterans Affairs survey of 517 companies classified as "pharmaceutical firms," "pharmaceutical, other firms," and "medical-surgical firms." As of August 1, of the 186 "pharmaceutical firms" that responded to the survey, 30 percent reported that they were Year 2000 compliant. Of the 72 "pharmaceutical, other firms" that responded to the survey, 39 percent were compliant. Finally, of the 259 "medical-surgical firms" that responded, 56 percent reported that they were compliant.

⁷⁶GAO/T-AIMD-00-39, October 28, 1999.

International: In addition to the risks associated with the nation's key economic sectors, one of the largest and most uncertain areas of risk relates to the global nature of the problem. On October 21, we testified that through its leadership of the President's Council's International Relations Working Group, the State Department has 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.⁷⁷ Similarly, we found that the U.S. Agency for International Development had devoted resources to assessing what Year 2000 problems could occur at many of its worldwide missions and on projects that it has funded that are currently underway within the countries where these missions are located. The collective efforts of State and the U.S. Agency for International Development to analyze international Year 2000 readiness have shown that some countries will simply not make their Year 2000 deadlines and, in fact, are likely to suffer disruptions in critical infrastructure-related services such as power, water, and finance.

The impact of Year 2000-induced failures in foreign countries could adversely affect the United States, particularly as it relates to the supply chain. To address the international supply chain issue, in January 1999 we suggested⁷⁸ that the President's Council on Year 2000 Conversion prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector, identify options for obtaining these materials through alternative avenues in the event that Year 2000-induced failures in the other country or in the transportation sector prevent these items from reaching the United States. In commenting on this suggestion, the Chair stated that the Council had (1) worked with federal agencies to identify sectors with the greatest dependence on international trade, (2) held industry roundtable discussions with the pharmaceutical and food supply sectors, and (3) hosted bilateral and trilateral meetings with the Council's counterparts in Canada and Mexico—the United States' largest trading partners.

In summary, while much improvement has been shown, additional work remains at the national, federal, state, and local levels to ensure that major

⁷⁷*Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning* (GAO/T-AIMD-00-25, October 21, 1999).

⁷⁸GAO/T-AIMD-99-50, January 20, 1999.

service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans and Day One strategies developed and validated. Similar actions remain to be completed by the nation's key sectors. Whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

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

Contacts

For information about this testimony, please contact Joel Willemsen at (202) 512-6253 or by e-mail at willemsenj.aimd@gao.gov.

GAO Reports and Testimony Addressing the Year 2000 Crisis

Overall Year 2000 Issues

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)

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

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

Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 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: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

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

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)

Banking and Finance

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

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

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: 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)

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

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

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)

Telecommunications

Year 2000 Computing Crisis: Readiness of the Telecommunications Industry (GAO/AIMD-99-293, September 30, 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: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

Power Generation and Distribution

Y2K Computing Challenge: Nuclear Power Industry Reported Nearly Ready; More Risk Reduction Measures Can Be Taken (GAO/T-AIMD-00-27, October 26, 1999)

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

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

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

Safety and Emergency Services

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

Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning (GAO/AIMD-00-8, October 14, 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: 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: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Water

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

Transportation

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

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

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

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

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

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

Health

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

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

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

Year 2000 Computing Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 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 Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 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 Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

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

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)

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

Revenue Collection

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 Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 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: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

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

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

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

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

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

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

Benefit Payments

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: Readiness of USDA High-Impact Programs Improving, But More Action Is Needed (GAO/AIMD-99-284, September 30, 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: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 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 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: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

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

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

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

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

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

National Security

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)

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

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

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

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

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

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

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

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

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

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

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)

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)

Other Government Services

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

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, 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 Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 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: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

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

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

**State and Local
Government**

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

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)

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)

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)

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

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

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

Cross-Cutting Issues

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

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

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

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

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

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

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 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: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

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

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

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

Appendix I
GAO Reports and Testimony Addressing the
Year 2000 Crisis

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

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

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Mail Postage & Fees Paid GAO Permit No. GI00</p>
