

GAO

Testimony

Before the Committee on Government Reform and the
Committee on Science, House of Representatives

For Release on Delivery
Expected at
11:15 a.m.
Wednesday,
January 20, 1999

**YEAR 2000 COMPUTING
CRISIS**

**Readiness Improving, But
Much Work Remains to
Avoid Major Disruptions**

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



Messrs. Chairmen and Members of the Committees:

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 Should these systems--which perform functions and services critical to our nation--suffer problems, it could create widespread disruption. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike.

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 as a high-risk area for the federal government.² Since that time, we have issued over 70 reports and testimony statements detailing specific findings and 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

Today, I will highlight the Year 2000 risks facing the nation, discuss the federal government's progress and remaining challenges in correcting its systems, identify state and local government Year 2000 issues, and provide an overview of the available information on the readiness of key public infrastructure and economic sectors.

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

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

³A list of these publications is included as an attachment to this statement.

⁴Year 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), which addresses the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); 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), which describes the tasks needed to ensure the continuity of agency operations; and 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), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

The Public Faces Risks of Year 2000 Disruptions

The public faces a risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. 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. Key sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The following are examples of some of the major disruptions the public and private sectors could experience if the Year 2000 problem is not corrected.

- With respect to aviation, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.⁵
- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Further, the Department of Defense could incur shortages of vital items needed to sustain military operations and readiness.⁶
- According to the Basle Committee on Banking Supervision--an international committee of banking supervisory authorities--failure to address the Year 2000 issue would cause banking institutions to experience operational problems or even bankruptcy.
- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if their software applications or embedded chips use two-digit fields to represent the year.

Recognizing the seriousness of the Year 2000 problem, on February 4, 1998, the President signed an executive order that established the President's Council on Year 2000 Conversion led by an Assistant to the President and consisting of one representative from each of the executive departments

⁵FAA Systems: *Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems* (GAO/T-AIMD-98-251, August 6, 1998).

⁶Defense Computers: *Year 2000 Computer Problems Threaten DOD Operations* (GAO/AIMD-98-72, April 30, 1998).

and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies, (2) acting as chief spokesperson in national and international forums, (3) providing policy coordination of executive branch activities with state, local, and tribal governments, and (4) promoting appropriate federal roles with respect to private-sector activities.

Much Work Remains to Address the Federal Government's Year 2000 Problem

Addressing the Year 2000 problem will be a tremendous challenge for the federal government. Many of the federal government's computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages, many of which are obsolete. Some applications include thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems.

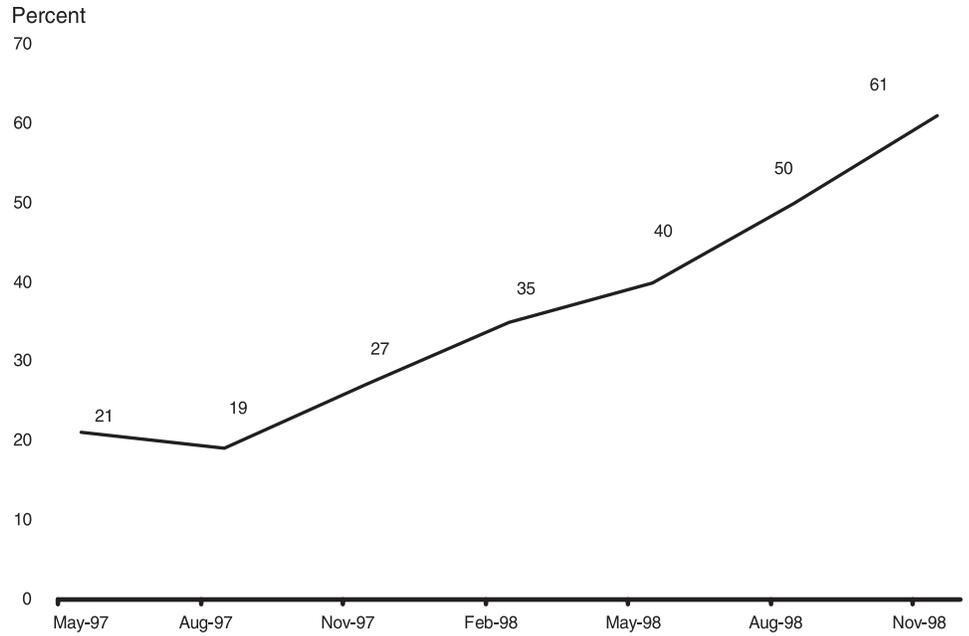
To meet this challenge and monitor individual agency efforts, the Office of Management and Budget (OMB) directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as business continuity and contingency plans and costs.

Latest Quarterly Reports Show Some Improvement, But More Work Is Needed

While the federal government's most recent reports show improvement in addressing the Year 2000 problem, 39 percent of mission-critical systems were reported as not yet compliant. As figure 1 illustrates, in May 1997, OMB reported that about 21 percent of the mission-critical systems (1,598 of 7,649) for the 24 major departments and agencies were Year 2000 compliant.⁷ Eighteen months later, OMB reported that, as of mid-November 1998, 4,069 of the 6,696 mission-critical systems in their current inventories, or about 61 percent, were compliant.

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

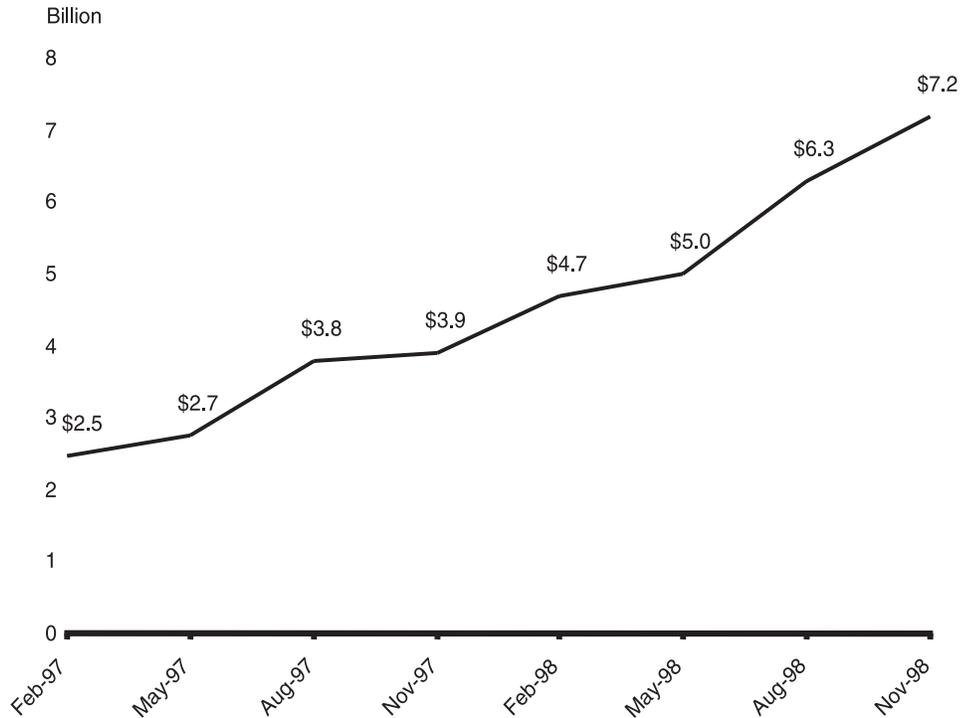
Figure 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997- November 1998



Source: OMB quarterly reports.

As federal agencies have more fully realized the complexities and extent of Year 2000 activities, estimated costs have also continued to rise. As figure 2 illustrates, since February 1997, the federal government's Year 2000 cost estimate has more than tripled.

Figure 2: Federal Government's Year 2000 Estimated Costs (Dollars in Billions)



Note: The August 1998 figure of \$6.3 billion and the November 1998 figure of \$7.2 billion are the totals of all individual submissions from the 24 major departments and agencies that were generally submitted on August 14th and November 13th, respectively. In its summaries of the agency reports, OMB reported the government's total estimated Year 2000 costs as \$5.4 billion and \$6.4 billion, respectively. For the August 1998 costs, OMB did not include all costs in its estimate because, for example, it was still reviewing some of the estimates provided by the agencies. For the November 1998 costs, OMB did not provide explanations in its report for the discrepancies between the agency reports and its estimates for 15 of the 18 agencies with differences.

Source: February 1997 data are from OMB's report Getting Federal Computers Ready for 2000, February 6, 1997. May 1997 through May 1998 data are from OMB's quarterly reports. The August and November 1998 data are from the quarterly reports of the 24 major federal departments and agencies.

In addition, many agencies have not met, or are at high risk of not meeting, OMB's interim target dates for completing assessment, renovation, and validation of systems to be repaired. As of mid-November 1998,

- 4 of the 24 major departments and agencies (17 percent) reported that they had not completed assessing their mission-critical systems to be repaired--over a year behind OMB's governmentwide target of June 1997,

-
- 16 of the 24 major departments and agencies (67 percent) reported that they had not completed renovating their mission-critical systems to be repaired--several weeks after OMB's governmentwide deadline of September 1998, and
 - 6 of the 24 major departments and agencies (25 percent) reported that they had validated 50 percent or fewer of their mission-critical systems to be repaired (OMB's governmentwide target to complete validation is January 1999).

Federal agencies must also be concerned about the Year 2000 readiness of their telecommunications and embedded systems. However, according to the 24 major departments' and agencies' November 1998 quarterly reports, many agencies had not completed inventorying and/or assessing their telecommunications or embedded systems.

Many federal agencies that are trying to cope with this enormous task are also facing concerns about whether they have sufficient staff. As we reported in April 1998⁸ and again in October 1998,⁹ many agencies have expressed concerns that the personnel needed to resolve their Year 2000 problems would not be available. However, comments from these agencies are largely anecdotal, and a comprehensive, analytical assessment of the issue has not yet been made. As a result, the full extent and severity of the Year 2000 workforce issue across the government is not known. The President's Council on Year 2000 Conversion, the Office of Personnel Management (OPM), and the Chief Information Officers (CIO) Council have various initiatives underway to address Year 2000 personnel issues. However, it is not yet known whether these efforts will ensure an adequate supply of qualified personnel to solve the government's Year 2000 problem.

Among our recommendations on this issue was that OMB determine if recent OPM initiatives have satisfactorily addressed agencies' reported personnel problems and, if they have not, designate an official to work with OPM and the CIO Council to help individual agencies resolve their Year 2000 workforce concerns. The Chair of the President's Council on Year 2000 Conversion and officials representing the CIO Council, OMB, and OPM concurred with our recommendations.

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

⁹Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998).

Reviews Show Uneven Federal Agency Progress

While the Year 2000 readiness of the government has improved, our reviews of federal agency Year 2000 programs have found uneven progress. Some agencies are significantly behind schedule and are at high risk that they will not fix their systems in time. Other agencies have made progress, although risks continue and a great deal of work remains.

Overall, our more than 70 reports and testimony statements contained over 100 recommendations related to the Year 2000 readiness of a wide range of individual agencies. These recommendations have been almost universally embraced.

Our recommendations have centered on the following.

- **Project planning.** We have recommended better organizational planning and management oversight--including systems inventorying and analysis--in a number of programs and entities.
- **Priority-setting.** With over 2,600 mission-critical systems still needing to be made Year 2000 compliant, it is important to establish priorities. Resources need to be focused on those business processes and supporting systems that could threaten national security, the economy, the health and safety of Americans, or their financial well-being.
- **Data exchanges.** To remediate their data exchanges, agencies must (1) identify data exchanges that are not Year 2000 compliant, (2) reach agreement with exchange partners (such as states) on the date format to be used, (3) determine if data bridges and filters are needed and, if so, reach agreement on their development,¹⁰ (4) develop and test such bridges and filters, and (5) test and implement new exchange formats.
- **Testing.** Agencies should perform thorough testing of their systems, including end-to-end testing of multiple systems supporting a major business function.
- **Business continuity and contingency planning.** Given the interdependencies among agencies, their business partners, and the public infrastructure, 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.

The following are examples of the results of some of our recent reviews.

¹⁰A bridge is used to convert two-digit years to four-digit years or to convert four-digit years to two-digit years. A filter is used to screen and identify incoming noncompliant data to prevent them from corrupting data in the receiving system.

-
- In September 1998, we reported¹¹ that the Health Care Financing Administration (HCFA) had taken several steps to respond to recommendations in our May 1997 report in which we identified serious problems in HCFA's oversight of its Medicare contractors' Year 2000 remediation efforts, as well as problems with its own Year 2000 activities.¹² At that time, however, HCFA and its contractors were severely behind schedule in repairing, testing, and implementing the mission-critical systems supporting Medicare. As a result, in September, we concluded that it was highly unlikely that all of the Medicare systems would be compliant in time to ensure the delivery of uninterrupted benefits and services into the year 2000. To improve the prospects for success, we made several recommendations to HCFA, including the need to rank the remaining Year 2000 work on the basis of an integrated project schedule. We further recommended that HCFA (1) identify the critical path for its Year 2000 program to ensure that all critical tasks are prioritized and completed in time to prevent unnecessary delays, (2) define the scope of an end-to-end test of the Medicare claims process and develop plans and a schedule for conducting such a test, (3) develop a risk management process, and (4) accelerate the development of business continuity and contingency plans for the Medicare program. HCFA has agreed to implement these recommendations.
 - In August 1998, we reported¹³ that the Department of Veterans Affairs had made progress in addressing the Year 2000 recommendations in our May 1997 report.¹⁴ However, concerns remained, including that (1) the Veterans Benefits Administration had made limited progress in renovating two key mission-critical systems--one that processes claims benefits and updates benefits information, and one that contains veterans' names, addresses, service histories, and claims folder locations--and (2) the Veterans Health Administration did not know the full extent of its Year 2000 problem because it had not yet completed its assessment of, for example, locally developed software or customized versions of national applications used by its medical facilities. We made

¹¹Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

¹²Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997).

¹³Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998).

¹⁴Veterans Benefits Computer Systems: Risks of VBA's Year 2000 Efforts (GAO/AIMD-97-79, May 30, 1997).

additional recommendations to the Department of Veterans Affairs, including that it (1) reassess its Year 2000 mission-critical efforts for the two key mission-critical systems where limited progress had been made as well as other information technology projects to ensure that Year 2000 efforts have adequate resources to achieve compliance in time and (2) ensure the rapid development of business continuity and contingency plans for each medical facility.

- Our work has shown that the Department of Defense (DOD) and the military services face significant problems.¹⁵ For example, our June 1998 report on the Navy found that while positive actions have been taken, remediation progress had been slow and the Navy was behind schedule in completing the early phases of its Year 2000 program.¹⁶ Further, the Navy had not been effectively overseeing and managing its Year 2000 efforts and lacked complete and reliable information on its systems and on the status and cost of its remediation activities. We recommended improvements to DOD and the military services' Year 2000 programs related to critical issues such as data exchanges, testing, and contingency planning; they have concurred with these recommendations.

In addition to our agency-specific reports, in April 1998, we highlighted governmentwide vulnerabilities and made recommendations to the President's Council on Year 2000 Conversion to address them.¹⁷

Verification Strategy

OMB's assessment of the current status of federal Year 2000 progress was predominantly based on agency reports that had not been consistently reviewed or verified. Without independent reviews, OMB and the President's Council on Year 2000 Conversion had little assurance that they were receiving accurate information. In fact, we have found cases in which agencies' systems compliance status as reported to OMB has been inaccurate. For example, in June 1998, the DOD Inspector General estimated that almost three quarters of DOD's mission-critical systems reported as compliant in November 1997 had not been certified as

¹⁵Defense 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); GAO/AIMD-98-72, April 30, 1998; and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

¹⁶GAO/AIMD-98-150, June 30, 1998.

¹⁷GAO/AIMD-98-85, April 30, 1998.

compliant by DOD components.¹⁸ In May 1998, the Department of Agriculture reported 15 systems as compliant, even though these were replacement systems that were still under development or were planned for development.¹⁹ (The department removed these systems from compliant status in its August 1998 quarterly report.)

To address this issue, we previously recommended that the Council require agencies to develop an independent verification strategy. According to OMB, all agencies are now required to independently verify their validation process and senior management at all large agencies are now relying on independent verification to provide a double-check that their mission-critical systems will, in fact, be ready for the year 2000.

One tool that some agencies are using to ensure the compliance of their mission-critical systems is a certification process. For example, in August 1998, a Deputy Secretary of Defense memorandum required that the Chief of Staff of the Army, Chief of Naval Operations, Chief of Staff of the Air Force, Commandant of the Marine Corps, and the Directors of the Defense Agencies certify that they have tested the Year 2000 capabilities of their respective components and national security systems. Such a certification, signed by the agency head, would reemphasize that the agency head is accountable for ensuring that the organization's mission-critical systems are Year 2000 compliant and could also provide a higher degree of confidence and valuable reassurance that a system reported as compliant has been comprehensively remediated and tested.

End-to-End Testing

To ensure that their mission-critical systems can reliably exchange data with other systems and that they are protected from errors that can be introduced by external systems, agencies must perform end-to-end testing of their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, 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--is

¹⁸Year 2000 Certification of Mission-Critical DOD Information Technology Systems (DOD Office of the Inspector General, Report No. 98-147, June 5, 1998).

¹⁹Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998).

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).²⁰ We recommended that for the highest priority functions, the Council designate lead agencies responsible for ensuring that end-to-end operational testing of processes and supporting systems is performed.

Some of this type of testing has been performed in the government. However, lead agencies have not been designated to take responsibility for ensuring that end-to-end testing of processes and supporting systems is performed across boundaries, and that independent verification and validation of such testing is ensured.

Business Continuity and Contingency Planning

Business continuity and contingency plans are essential. Without such plans, when unpredicted 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, we recommended that the Council require agencies to develop contingency plans for all critical core business processes. Since early 1998, OMB has clarified its contingency plan instructions and, along with the CIO Council, has adopted our business continuity and contingency planning guide.²¹ In the case of the 24 major departments and agencies, we reported in March 1998²² that--according to their February 1998 quarterly reports--several agencies planned to develop contingency plans only if they fell

²⁰GAO/AIMD-10.1.21, November 1998.

²¹GAO/AIMD-10.1.19, August 1998.

²²Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998).

behind schedule in completing their Year 2000 fixes. As we testified in June 1998,²³ only limited progress was reported in agencies' May 1998 quarterly reports, which indicated that only four agencies had drafted contingency plans for their core business processes. According to their latest quarterly reports in November 1998, many agencies reported that they had completed or are drafting Year 2000 contingency plans for the continuity of their core business processes while others were in the early stages of such planning.

A key aspect of business continuity and contingency planning is testing the plan to evaluate whether individual contingency plans are capable of providing the level of support to the agency's core business processes and whether the plan can be implemented within a specified period of time. In instances in which a full-scale test may not be feasible, the agency may consider end-to-end testing of key plan components. Moreover, an independent review of the plan can validate the soundness of the proposed contingency strategy. To provide assurance that agencies' business continuity and contingency plans will work if they are needed, OMB may want to consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.

As noted in our business continuity and contingency guide,²⁴ another key element of a business continuity and contingency plan is the development of a zero day or day one risk reduction strategy, and procedures for the period from late December 1999 through early January 2000. For example, the Social Security Administration (SSA)--a recognized federal leader in addressing the Year 2000 issue--has developed such a strategy. Among the features of this strategy is a moratorium on software changes, except for those mandated by law. SSA plans to minimize changes to its systems that have been certified as Year 2000 compliant by not allowing discretionary changes to be made. The moratorium will be in effect for commercial-off-the-shelf and mainframe products from July 1, 1999 through March 31, 2000, and for programmatic applications from September 1, 1999 through March 31, 2000. Such a Year 2000 change management policy will significantly reduce the chance that errors will be introduced into systems that have already been found to be compliant. Because this policy can

²³Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998).

²⁴GAO/AIMD-10.1.19, August 1998.

reduce agencies' risks, OMB may want to consider directing agencies to implement similar policies.

Other aspects of SSA's day one strategy are the implementation of (1) an integrated control center, whose purposes include the internal dissemination of critical data and problem management, and (2) a timeline that details the hours in which certain events will occur (such as when workloads will be placed in the queue and backup generators will be started) during the late December and early January rollover period. OMB may wish to consider requiring other agencies to develop similar plans.

SSA is also planning to address the personnel issue with respect to the rollover. For example, it plans to obtain a commitment from key staff to be available during the rollover period and establish a Year 2000 leave policy. Such a strategy, developed well in advance of the turn of the century, would help agencies manage the risks associated with the actual rollover and better position agencies to address disruptions if they occur. Therefore, OMB may wish to consider requiring agencies to develop and implement similar plans for the change of century rollover.

Reporting of Year 2000 Progress

To improve oversight of Year 2000 readiness, we previously recommended changes to OMB's quarterly reporting process. Specifically, we recommended (1) requiring additional agencies that play a significant role in the life of the nation to also report regularly to OMB, (2) requiring agencies to report on the status of their efforts to replace systems, not just on those being renovated, and (3) specifying the particular steps that must be taken to complete each phase of a Year 2000 program (i.e., assessment, renovation, validation, and implementation).

OMB has acted on these recommendations. Specifically, on March 9 and April 21, 1998, OMB issued memorandums to an additional 31 and 10 agencies, respectively, requiring that they provide information on their Year 2000 progress and again in about a year's time (beginning with the August 1998 report, OMB required nine of these agencies to report quarterly). In addition, in its April 28, 1998, quarterly reporting guidance, OMB requested that agencies provide information on the oversight mechanism(s) used to ensure that replacement systems are on schedule; it also specified that agencies should ensure that their reporting on the completion of phases be consistent with the CIO Council's best practices guide and our enterprise

readiness guide.²⁵ Moreover, in June 1998, OMB required that agencies that were not making adequate progress or about which OMB had concerns report monthly on their progress in remediating mission-critical systems.

While these initiatives have enhanced the government's understanding of its Year 2000 remediation status, OMB has an opportunity to further improve its reporting approach. OMB's draft guidance for the next quarterly reports is a good first step towards improving this approach. OMB's draft guidance calls on federal agencies to identify and report on the core business functions that are to be addressed in their business continuity and contingency plans. We endorse this initiative because it could help identify the government's critical functions.

OMB could go a step further and require that agencies, based on their core business functions, report on the status of their end-to-end testing and business continuity and contingency plans.

- **End-to-end testing.** The boundaries on end-to-end tests are not fixed or predetermined, but rather vary depending on a given business area's system dependencies (internal and external) and criticality to the mission of the organization. Therefore, in planning end-to-end tests, a critical step is to understand and analyze the organization's core business functions. In addition, such critical business functions often involve multiple mission-critical systems that cut across organizational boundaries. With the time available for end-to-end testing diminishing, we believe that OMB should consider, for the government's most critical functions, setting target dates, and having agencies report against them, for the development of end-to-end test plans, the establishment of test schedules, and the completion of the tests.
- **Business Continuity and Contingency Planning.** The identification of core business functions is a necessary feature of a business continuity and contingency plan. If agencies are required to identify these functions in the February 1999 quarterly report, OMB could consider setting a target date, such as April 30, 1999, for the completion of business continuity and contingency plans, and require agencies to report on their progress against this milestone. This would encourage agencies to expeditiously develop and finalize their plans and would provide the Council and OMB with more complete information on agencies' status on this critical issue.

²⁵GAO/AIMD-10.1.14, September 1997.

Another key task that could be aided by the identification of the government's core business functions is setting priorities. While individual agencies have been identifying mission-critical systems, this has not always been done on the basis of a determination of the agency's most critical operations. Governmentwide priorities need to be 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. Further, if priorities are not clearly set, the government may well end up wasting limited time and resources in fixing systems that have little bearing on the most vital government operations. Other entities have recognized the need to set priorities. For example, Canada established 48 national priorities covering areas such as national defense, food production, safety, and income security. In April 1998, we recommended that the Council establish governmentwide priorities and ensure that agencies set agencywide priorities. However, governmentwide priorities have not yet been established. Identification of the government's core business functions provides an opportunity to do this.

State and Local Governments Face Significant Year 2000 Risks

State and local governments also face a major risk of Year 2000-induced failures to the many vital services that they provide. For example,

- food stamps and other types of payments may not be made or could be made for incorrect amounts;
- date-dependent signal timing patterns could be incorrectly implemented at highway intersections, and safety severely compromised, if traffic signal systems run by state and local governments do not process four-digit years correctly; and
- prisoner release or parole eligibility determinations may be adversely affected by the Year 2000 problem.

A recent survey of state Year 2000 efforts indicated that much remains to be completed. The states reported to the National Association of State Information Resource Executives that, as of January 15, 1999,²⁶ they had

²⁶Individual states submit periodic updates to the National Association of State Information Resource Executives. For the January 15th report, the states submitted their data from December 7, 1998 through January 14, 1999.

thousands of mission-critical systems.²⁷ With respect to the remediation of these systems, (1) 9 states reported that they had completed between 1 and 24 percent of the activities required to return a modified system or renovated process to production, (2) 12 states reported completing between 25 and 49 percent, (3) 19 states reported completing between 50 and 74 percent, and (4) 6 states reported completing more than 75 percent of their mission-critical systems.²⁸ On a more positive note, almost all states reported that they are actively engaged in internal and external contingency planing. However, of the 48 states that established target dates for the completion of these plans, 16 (33 percent) reported the deadline as September 1999 or later.

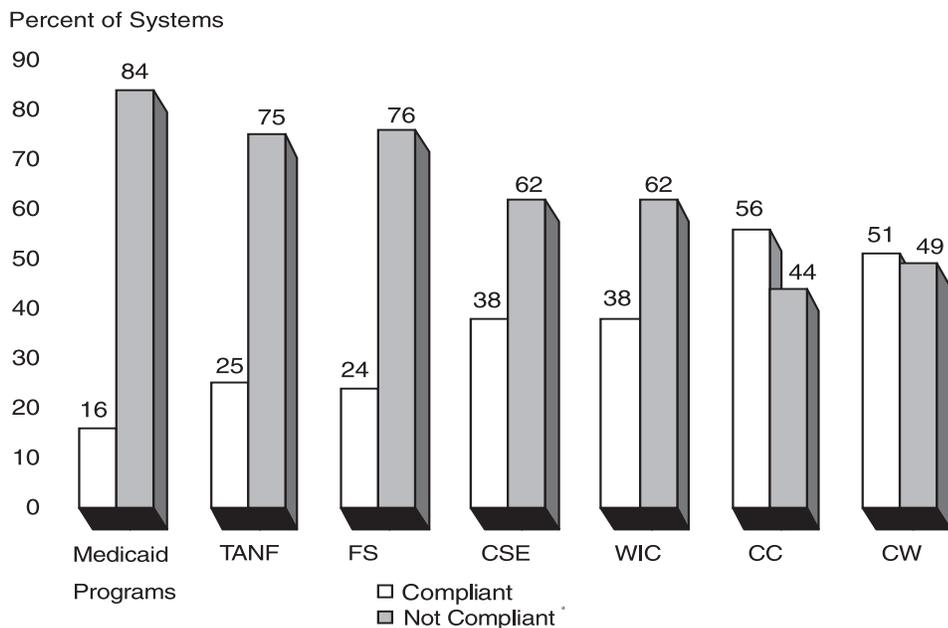
Our recent survey of the state systems used in federal welfare programs revealed that the majority of state welfare systems were not yet Year 2000 compliant (see figure 3).²⁹ Failure to complete Year 2000 conversion could result in billions of dollars in benefits payments not being delivered on time or in correct amounts. Other highlights of the survey results included that states reported that (1) assessment had been completed for about 80 percent of the welfare systems and (2) renovation had been completed on about one-third of the welfare systems.

²⁷The National Association of State Information Resource Executives defined mission-critical systems as those that the state has identified as priorities for prompt remediation.

²⁸Four states did not respond to this question.

²⁹Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998). The survey was conducted in July and August 1998 and included the following welfare programs: Medicaid; Temporary Assistance for Needy Families (TANF); Women, Infants, and Children (WIC); food stamps (FS); child support enforcement (CSE); child care (CC); and child welfare (CW). Forty-nine states, the District of Columbia, and three territories responded to our survey.

Figure 3: Reported Status of State Welfare Systems, as of July/August 1998



^aIn some cases, systems reported as compliant have not been validated.

State audit organizations have identified other significant Year 2000 concerns. For example, (1) California's State Auditor reported³⁰ that state agencies were prematurely declaring their critical projects complete when they had not been thoroughly tested, that not all state agencies had completed the necessary steps to ensure that data exchanges will work seamlessly, and that managers of most state agencies had not developed business continuity plans, (2) Texas' Office of the State Auditor reported³¹ that many state entities had not finished their embedded systems inventories and, therefore, it was not likely that they would complete their embedded systems repairs before the year 2000, and (3) Vermont's Office of Auditor of Accounts reported³² that the state faces the risk that critical

³⁰Year 2000 Computer Problem: Progress May Be Overly Optimistic and Certain Implications Have Not Been Addressed (August 27, 1998).

³¹A Review of Oversight for the State's Embedded Systems Year 2000 Repair Efforts (SAO Report No. 98-056, August 10, 1998).

³²State Auditor's Report On Vermont's Year 2000 Preparedness For The Period Ending April 1, 1998 (May 5, 1998).

portions of its Year 2000 compliance efforts could fail. State audit offices have also made recommendations, including the need for increased oversight, Year 2000 project plans, contingency plans, and personnel recruitment and retention strategies.

Recent reports on local governments have also highlighted significant Year 2000 concerns at this level. For example,

- A November 1998 survey commissioned by the National Association of Counties of a sample of 500 counties found that (1) 50 percent of the counties had a countywide Year 2000 plan, (2) 36 percent had completed assessment, (3) 16 percent had repaired or replaced their systems, (4) 41 percent had completed an inventory of county equipment that contain embedded systems, (5) 28 percent planned to conduct countywide testing, and (6) 73 percent had no contingency plans.
- Our testimony³³ on the District of Columbia reported that while the pace of the District's Year 2000 effort had picked up considerably, the District is still far behind in addressing the problem and at risk that critical processes could fail. Vital activities that the District should undertake include promptly identifying its most important operations and determining which systems supporting these operations can be fixed before the Year 2000 deadline.
- Among the Pennsylvania's Legislative Budget and Finance Committee's recent findings regarding its local government entities were that (1) many have not attempted to identify if they have a Year 2000 problem, (2) they appear largely unaware of potential embedded system problems, and (3) less than half of the entities that contract with service vendors have received verbal or written assurance that their vendors' systems will be Year 2000 compliant.³⁴
- The Office of the New York State Comptroller's Division of Municipal Affairs reported that while 100 percent of New York's counties had made plans to deal with the Year 2000 problem, 26 percent of the cities, 54 percent of the towns, 48 percent of the villages, and 61 percent of the fire districts had not made plans to address the Year 2000 problem.³⁵

³³Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998).

³⁴The Year 2000 Problem in Local Governments and School Districts (September 1998).

³⁵1998 Municipal Technology Survey Results (September 1998).

The Chair of the President's Council on Year 2000 Conversion has expressed concerns about the Year 2000 readiness of state and local governments and has developed initiatives to address them. For example, the Council established working groups on state and local governments and tribal governments. The Chair of the Council also participates in monthly multistate conference calls. In addition, OMB's draft guidance for the next quarterly reports requires federal agencies to report on the status of states that administer federal programs. This is an important initiative because states are key to the federal government's implementation of certain critical programs (such as food stamps and Medicaid). Accordingly, we also believe that OMB may want to consider establishing Year 2000 target dates (such as when renovation, validation, and implementation should be completed) for states to meet. In addition, OMB should consider ensuring that agencies have developed business continuity and contingency plans for state-administered programs that would be implemented if a state does not meet certain milestones.

The extent of information available to the public on state and locality Year 2000 readiness varies considerably. For example, while some states and local governments provide detailed Year 2000 readiness information on their web sites, others provide only limited data. States that are providing detailed readiness information are assisting their citizens in understanding the progress being made to address the Year 2000 problem. Accordingly, another initiative that the Council could consider is developing and distributing to state and local governments a template that identifies the types of Year 2000 information that the entity could disclose to the public. For example, the template could contain the percentage of systems that the state or local government has assessed, renovated, and validated in key areas such as utilities, transportation, health and human services, safety and emergency services, revenue, education, and administrative systems (such as elections systems). In areas in which the state or local government may perform a regulatory function, such as drinking water or electric power, the government could provide readiness data on those regulated entities. Public disclosure of such information could reduce the public's concern over potential disruptions caused by Year 2000-induced failures.

Year 2000 Readiness Information Available in Some Sectors, But Key Information Still Missing or Incomplete

Beyond the risks faced by the 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 Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.³⁶ 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 recently announced that he was forming a Senior Advisors Group composed 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. The first meeting of this group is scheduled for this month.

Our April 1998 report also recommended that the President's Council on Year 2000 Conversion develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic 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 Chair plans to issue quarterly public reports summarizing these assessments. The first such report was issued on January 7, 1999.

The January 7, 1999, report summarizes information collected to date by the working groups and various trade associations.³⁷ The Council acknowledged that readiness data in certain industries were not yet available and, therefore, were not included in the report. Nevertheless, based on the information available at the time, it concluded that

- virtually all of the industry areas reported high awareness of the year 2000 and its potential consequences;

³⁶GAO/AIMD-98-85, April 30, 1998.

³⁷First Quarterly Summary of Assessment Information (The President's Council on Year 2000 Conversion, January 7, 1999).

-
- participants in several areas, particularly financial institutions, are mounting aggressive efforts to combat the problem;
 - it is increasingly confident that there will not be large-scale disruptions in the banking, power, and telecommunications areas and, if disruptions do occur, they are likely to be localized;
 - large organizations often have a better handle on the Year 2000 problem than do smaller ones, and some small- and medium sized businesses and governments continue to believe that the Year 2000 problem will not affect them or are delaying action until failures occur; and
 - international failures are likely since, despite recent increased efforts, a number of countries have done little to remediate critical systems.

The Council's report is a good step toward obtaining a picture of the nation's Year 2000 readiness. However, the picture remains substantially incomplete because assessments were not available in many key areas, such as 911 centers, fire services, and the maritime industry. Also, some surveys did not have a high response rate, calling into question whether they accurately portray the readiness of the sector. In addition, in some cases, such as drinking water and health care, the report provides a general assessment of the sector but does not contain detailed data as to the status of the sector (e.g., the average percentage of organization's systems that are Year 2000 compliant or the percentage of organizations that are in the assessment, renovation, or validation phases).

The Council must remain vigilant and closely monitor and update the information in the sectors where information is available and obtain information for those where it is not. Particular attention should be paid to the public infrastructure, including critical areas such as power, water, and telecommunications, since most, if not all, major enterprises rely on these essential elements for daily functioning. Other key economic sectors include health, safety, and emergency services; banking and finance; transportation; and manufacturing and small business. In addition, with the advent of electronic communication and international commerce, the United States is also critically dependent on international Year 2000 readiness.

Power

The electric power industry is complex and highly automated. It is made up of an interconnected network of generation plants, transmission lines, and distribution facilities. There are three independent interconnections that provide electricity to every household and company in North America.

On January 11, 1999, the North American Electric Reliability Council (NERC) issued its second report on the Year 2000 status of electric power systems.³⁸ NERC found that, as of November 30, 1998, on average, the electric industry is close to, but slightly lagging in, meeting the industry's target date of June 30, 1999, for being "Year 2000 ready."³⁹ In addition, NERC reported that reporting organizations, on average, had completed 96 percent of the inventory phase, 82 percent of the assessment phase, and 44 percent of the remediation/testing phase.

Related to the power sector are the oil and gas industries. An August 1998 survey of these industries by the President's Council on Year 2000 Conversion's oil and gas working group, in conjunction with the American Petroleum Institute, the Interstate Natural Gas Association of America, the American Gas Association, and other industry groups found that for their business systems and associated software, (1) 45 percent of respondents⁴⁰ were in the planning, inventory, or assessment phases, (2) 36 percent were in the remediation phase, and (3) 19 percent were in the validation phase. In regard to embedded systems, (1) 60 percent of respondents were in the planning, inventory, or assessment phases, (2) 26 percent were in the remediation phase, and (3) 14 percent were in the validation phase.

Water

The water sector includes drinking water and wastewater utilities. These utilities are owned by local governments and private companies and range in size from small, serving communities of less than 10,000, to large, serving populations of over 1 million. Automation in these utilities varies greatly as well, from plants with high levels of automation to smaller plants with little, if any, computerized equipment.

³⁸Preparing the Electric Power Systems of North America for Transition to the Year 2000 (NERC, January 11, 1999). This report was prepared in response to a May 1998 request by the Department of Energy. According to NERC, about 98 percent of the electricity supply and delivery organizations in North America participated in this assessment (194 of 198 bulk electric entities and 2,821 of 2,888 distribution entities).

³⁹NERC defined Year 2000 ready as meaning that a system or component has been determined to be "suitable for continued use into the Year 2000." NERC noted that "this is not necessarily the same as Y2K Compliant, which implies fully correct date manipulations."

⁴⁰The respondents to this survey represented 45 percent of U.S. oil and natural gas production, 78 percent of U.S. refining capacity, 70 percent of U.S. crude oil and refined product pipeline deliveries, 81 percent of natural gas interstate pipeline deliveries, 43 percent of U.S. branded retail outlets, and 50 percent of the total natural gas volume of investor-owned local distribution companies.

A September 1998 report on a survey by the American Water Works Association, the Association of Metropolitan Water Agencies, and the National Association of Water Companies⁴¹ stated that of the 600 responding public water utilities, half had completed their assessments of internal systems. These organizations expect to complete a more extensive report on the readiness of water system operators by March 1999. With respect to wastewater systems, in December 1998, the Association of Metropolitan Sewage Agencies reported that 95 percent of respondents⁴² had begun to implement solutions for the Year 2000 problem, while 26 percent were complete or nearly complete.

Telecommunications

In testimony in June, we reported that the Year 2000 readiness of the telecommunications sector is one of the most crucial concerns to our nation because telecommunications are critical to the operation of nearly every public- and private-sector organization.⁴³ For example, the information and telecommunications sector (1) enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems, (2) is essential to the service economy, manufacturing, and efficient delivery of raw materials and finished goods, and (3) is basic to responsive emergency services. Reliable telecommunications services are made possible by a complex web of highly interconnected networks supported by national and local carriers and service providers, equipment manufacturers and suppliers, and customers.

According to the President's Council on Year 2000 Conversion, information from the telecommunications industry indicates that the major companies have active Year 2000 programs and have made substantial progress toward updating their systems but that less information is available regarding the readiness of smaller organizations. With respect to specific segments of the telecommunications sector, (1) preliminary information from the Network Reliability and Interoperability Council found that based on a

⁴¹These organizations represent approximately 4,000 public water systems, which provide services to about 80 percent of the United States population.

⁴²The Association of Metropolitan Sewage Agencies originally surveyed its 206 members in June 1998 and conducted a follow-up survey in October 1998. Seventy-six agencies responded to the June survey and 43 responded to the October follow-up.

⁴³Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998).

polling of companies that represent 94 percent of the access lines in the United States, the average target completion date was June 30, 1999, (2) current data are not available for the cable segment but responses to a survey by the Cable Services Bureau are expected in early 1999, (3) the Wireless Telecommunications Bureau expects to complete a comprehensive assessment of this segment in the first quarter of 1999, and (4) the Mass Media Bureau is conducting a survey of a cross section of broadcasters that is expected to be completed in early 1999.

Health

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. Readiness information on the health care sector has been limited. However, the Council's health care working group plans to gather Year 2000 readiness information of this sector throughout 1999, especially among smaller health care organizations. In addition, with the support of the Association of State and Territorial Health Officials, the Centers for Disease Control and Prevention sent a Year 2000 readiness assessment survey to 57 state and territorial health officials. The results of this survey are expected by the end of January 1999. In addition, the Department of Health and Human Services' Office of Inspector General plans to survey the Year 2000 readiness of a sample of Medicare providers.

We also have previously reported that HCFA and its contractors were severely behind schedule in repairing, testing, and implementing the mission-critical systems supporting Medicare.⁴⁴ In addition, our July/August 1998 survey of state Medicaid systems found that 16 percent were Year 2000 compliant.⁴⁵

Regarding biomedical equipment, we reported that the Department of Health and Human Services' Food and Drug Administration (FDA)--which provides information from the biomedical equipment manufacturers to the public through an Internet World Wide Web site--had no assurance that manufacturers had adequately addressed the Year 2000 problem for noncompliant equipment because it did not require manufacturers to

⁴⁴Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

⁴⁵Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

submit test results certifying compliance.⁴⁶ Moreover, FDA's database lacked detailed information on the make and model of compliant equipment and, as of July 30, 1998, only about 12 percent of biomedical equipment manufacturers had responded to FDA's inquiries. To address these issues, we recommended that the Departments of Health and Human Services and Veterans Affairs (1) work jointly to develop immediately a single data clearinghouse that provides compliance information to all users of biomedical equipment and (2) determine what actions, if any, should be taken regarding biomedical equipment manufacturers that have not provided compliance information.

In response to our recommendation, FDA, in conjunction with the Department of Veterans Affairs, established a biomedical equipment clearinghouse. The Department of Health and Human Services reported that, as of October 28, 1998, approximately two-thirds of the biomedical equipment manufacturers that make products containing electronic components have provided information to the clearinghouse.

Safety and Emergency Services

This sector involves organizations that respond to disasters as well as those that have a daily impact on public safety, such as police, fire, and emergency medical services. The Federal Emergency Management Agency conducted a survey of state emergency management directors in October/November 1998 and received responses from 46 states, the District of Columbia, and 4 territories. According to the Federal Emergency Management Agency, all state-level agencies have resolved, or planned to resolve, the vast number of Year 2000-related issues involving critical emergency preparedness facilities, systems, and services. Concerns were raised, however, about the limited amount of resources to assess, fix, test, and validate state-level systems. In addition, the state emergency management directors were not generally aware of the status of emergency preparedness and Year 2000 progress at the local level. A survey by the International Association of Emergency Managers, which has a membership of 1,700 individuals representing local emergency management organizations, found that of the 172 respondents, 159 were actively working on the Year 2000 problem and 59 reported that their systems were "fully prepared."

⁴⁶Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

Information on the Year 2000 status of other parts of this sector, such the readiness of fire services, 911 centers, emergency medical services, and local law enforcement, has not yet been collected although some assessments are ongoing or planned for early 1999.

Banking and Finance

A large portion of the institutions that make up the banking and finance sector are overseen by one or more federal regulatory agencies. In September 1998, we testified on the efforts of five federal financial regulatory agencies⁴⁷ to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.⁴⁸ We concluded that the regulators have made significant progress in assessing the readiness of member institutions and raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are 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.

With respect to the securities industry, a September 1998 Securities and Exchange Commission survey of the national securities exchanges, the National Association of Securities Dealers, the Securities Industry Association, and the registered or exempt clearing agencies found that (1) the exchanges and the National Association of Securities Dealers had completed remediation and testing on 95 percent of mission-critical systems and have finished implementation on 73 percent of these systems and (2) the clearing agencies have completed renovation and testing on 87 percent of critical systems and implementation of 86 percent of these systems.

Transportation

The transportation sector includes air traffic, railroads, the maritime industry, highways, and transit providers. We have previously expressed concern about the Federal Aviation Administration's (FAA) Year 2000

⁴⁷The 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.

⁴⁸Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

efforts. Specifically, we reported in August 1998,⁴⁹ that FAA had made progress in managing its Year 2000 problem and had completed critical steps in defining which systems needed to be corrected and how to accomplish this. However, with less than 17 months to go, FAA still had to correct, test, and implement many of its mission-critical systems. A November 1998 survey by the National Air Carrier Association, Inc. of its seven carriers that specialize in low-cost scheduled and charter passenger and cargo transportation had five respondents. The survey found that some of the small carriers had only 55 percent of their assessment completed, while larger carriers had made more progress. The results of surveys of larger commercial carriers and airports are expected in the first quarter of 1999.

According to the President's Council on Year 2000 Conversion, neither the railroad industry nor the maritime industry had complete, consolidated Year 2000 readiness assessment data although such information is expected in early 1999. A survey by the American Association of Motor Vehicle Administrators, which represents motor vehicle and traffic law enforcement administrators in the United States and Canada, received 44 responses from 31 states in an August 1998 survey. Thirty-four percent of respondents stated that they were Year 2000 compliant while 59 percent stated that they were assessing the issue or had at least one Year 2000 project planned or underway. With regard to transit providers, of the 162 respondents (a response rate of nearly 50 percent) to a American Public Transit Association May 1998 survey of transit systems, (1) 20 percent reported that they were Year 2000 compliant, (2) 79 percent reported that their systems would be Year 2000 compliant by the year 2000, and (3) 21 percent reported that they were not sure whether they would be compliant by the year 2000.

Manufacturing and Small Business

The manufacturing and small business sector includes the entities that produce or sell a myriad of products, such as electronics, heavy equipment, food, textiles, and automobiles. The President's Council on Year 2000 Conversion's consumer affairs working group is assessing the Year 2000 compliance of consumer products and financial services. In addition, the Federal Trade Commission, which chairs this working group, has set up a

⁴⁹FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

web site and the Council has established a toll-free telephone number through which consumers can obtain Year 2000 information.

The Department of Agriculture, the chair of the Council's food supply working group, contracted with the Gartner Group to obtain a Year 2000 assessment of the nation's food supply. The Gartner Group's analysis of the four largest companies within specific food industries (e.g., beef, refined sugar, and fertilizer) found that the awareness and progress of most of these companies was commendable and that remediation efforts ranged from still completing inventories and assessments to well underway. However, Gartner Group's research has shown that the level of preparedness of large companies is higher than that of smaller companies. Therefore, they cautioned that in food industries in which the large companies control only a small percentage of the market (such as the fish industry), an industrywide failure to remediate could have widespread impact.

The President's Council on Year 2000 Conversion reported that the status of Year 2000 efforts in the nation's millions of small- and medium-sized businesses is a concern. The National Federation of Independent Business reported in December 1998 on the results of its October/November survey of a sample of small businesses. According to this report, only 38 percent of respondents had taken or were taking action. In addition, according to the report, about one-third of small businesses that are aware of the Year 2000 problem and are vulnerable to it plan no preventive measures.

International

In addition to the risks associated with the nation's key economic sectors, one of the largest, and largely unknown, risks relates to the global nature of the problem. International concerns were underscored by a September 1998 report by the Organization for Economic Co-operation and Development.⁵⁰ This report stated that (1) while awareness is increasing, the amount of remediation still required is daunting, (2) significant negative economic impact is likely in the short term, although much uncertainty

⁵⁰The Organization for Economic Co-operation and Development surveyed its member countries and reviewed existing studies and media reports on the Year 2000 problem and issued a report on its findings, *The Year 2000 Problem: Impacts and Actions* (September 1998). The organization's 29 member countries are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

exists about the extent of Year 2000-induced disruptions, (3) governments face a major public management challenge requiring acceleration of their own preparations and stronger leadership, and (4) stronger international cooperation is essential, especially in conjunction with cross-border testing.

Another example of potential international problems is illustrated by a Gartner Group survey of 15,000 companies in 87 countries, which found that many countries are in the early stages of Year 2000 readiness. As of September 1998, the Gartner Group found that the United States, Australia, Belgium, Canada, England, Holland, Ireland, Sweden, and Switzerland were farthest ahead. Behind these leaders were countries such as Japan, Germany, India, and Brazil. Countries furthest behind included Russia, China, and the Philippines.⁵¹

The United States has attempted to promote international dialogue on the Year 2000 problem. In June 1998, the United Nations General Assembly adopted a resolution on the global implications of the Year 2000 issue. The resolution recognized that the Year 2000 issue threatened effective operation of governments, companies, and other organizations and coordinated efforts were required to address it. The resolution went on to request that all member countries attach a high priority to raising the level of awareness and to consider appointing a nationwide coordinator to tackle the problem. The Chair of the President's Council also has met with the United Nations and other international bodies, and helped organize a significant December 1998 National Y2K Coordinators' meeting attended by over 120 countries, hosted by the United Nations' Working Group on Informatics. This meeting should help encourage the establishment of regional coordinating mechanisms and foster greater international dialogue on the Year 2000 issue.

Additional Actions That Could Be Considered by the President's Council on Key Sectors

The President's Council on Year 2000 Conversion is to be commended on the strides that it has made to obtain Year 2000 readiness data that are critical to the nation's well-being as well as its other initiatives, such as the establishment of the Senior Advisors Group. To further reduce the

⁵¹Year 2000 Global State of Readiness and Risks to the General Business Community, testimony presented by the Gartner Group before the Special Committee on the Year 2000 Technology Problem, October 7, 1998.

likelihood of major disruptions, the Council may wish to consider other actions.

- The Council must continue to aggressively pursue readiness information in the areas in which it is lacking, such as the railroad industry, health sector, and local law enforcement. If the current approach of using associations to voluntarily collect information does not yield the necessary information, the Council may wish to consider whether legislative remedies (such as requiring disclosure of Year 2000 readiness data) should be proposed.
- To encourage the reporting of more complete information, the Council should consider requesting that the national associations publicly disclose, at a minimum, those companies that have responded to surveys.
- In its January 1999 meeting, the Chair provided Council members with items to consider when preparing the working groups' input into the April 1999 assessment report. These items included the key facts to obtain from survey information and information on the group conducting the assessment and number surveyed/number that responded. This type of data should help the Chair and the Council evaluate the readiness of the sectors. Indeed, we would urge the Council to include this same information in the April assessment report to the public. In addition, to ensure that the Council's working groups have adequately covered the nation's sectors, another goal for the next quarterly assessment report could be for the working groups to identify each sector's major components and report summary readiness information, including significant trends, by major component to the Chair for inclusion in the report to the public.
- Since the international arena carries some of the greatest Year 2000 risks and uncertainties, the Council could prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, and pharmaceuticals) and, working with the private sector (perhaps using the Senior Advisors Group), identify options to obtain these materials through alternative avenues in the event that Year 2000-induced failures in the importing country or in the transportation sector prevent these items from reaching the United States.

In summary, national, federal, state, and local efforts must increase substantially to ensure that major service disruptions do not occur. Strong leadership and partnerships are essential if government programs are to meet the needs of the public at the turn of the century.

Messrs. Chairmen, this concludes my statement. I would be happy to respond to any questions that you or other members of the Committees may have at this time.

GAO Reports and Testimony Addressing the Year 2000 Crisis

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

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

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

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

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

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

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

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

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

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

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

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

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain

(GAO/AIMD-98-248, September 17, 1998).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ordering Information

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

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

<http://www.gao.gov>

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

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

Address Correction Requested

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