United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
2 p.m.
Monday,
August 17, 1998

YEAR 2000 COMPUTING CRISIS

Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions

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

GAO/T-AIMD-98-266

Mr. Chairman and Members of the Subcommittee:

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 disruption, it could create a widespread crisis. 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 50 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 briefly discuss the Year 2000 risks facing the nation, highlight our major concerns with the federal government's progress in correcting its systems, identify state and local government Year 2000 issues, and discuss critical Year 2000 data exchange issues.

Risk of Year 2000 Disruption to the Public Is High

The public faces a high risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing crisis. 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

[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).

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

[4]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, 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, 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, Exposure Draft, June 1998), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions. Key economic 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 information and telecommunications sector is especially important. 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 operations of nearly every public-sector and private-sector organization.[5] 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.

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. With the advent of electronic communication and international commerce, the United States and the rest of the world have become critically dependent on computers. However, there are indications of Year 2000 readiness problems in the international arena. For example, in a June 1998 informal World Bank survey of foreign readiness, only 18 of 127 countries (14 percent) had a national Year 2000 program, 28 countries (22 percent) reported working on the problem, and 16 countries (13 percent) reported only awareness of the problem. No conclusive data were received from the remaining 65 countries surveyed (51 percent).

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.

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

- Unless the Federal Aviation Administration (FAA) takes much more decisive action, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.[6]
- 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 (DOD) could incur shortages of vital items needed to sustain military operations and readiness.[7]
- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if the computer systems, software applications, or embedded chips used in these devices contain two-digit fields for year representation.
- 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.

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 composed of one representative from each of the executive departments 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 Correct the Federal Government's Year 2000 Problem

Addressing the Year 2000 problem in time 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.

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

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

The federal government also depends on the telecommunications infrastructure to deliver a wide range of services. For example, the route of an electronic Medicare payment may traverse several networks—those operated by the Department of Health and Human Services, the Department of the Treasury's computer systems and networks, and the Federal Reserve's Fedwire electronic funds transfer system. In addition, the year 2000 could cause problems for the many facilities used by the federal government that were built or renovated within the last 20 years and contain embedded computer systems to control, monitor, or assist in operations. For example, building security systems, elevators, and air conditioning and heating equipment could malfunction or cease to operate.

Agencies cannot afford to neglect any of these issues. If they do, the impact of Year 2000 failures could be widespread, costly, and potentially disruptive to vital government operations worldwide. Nevertheless, overall, the government's 24 major departments and agencies are making slow progress in fixing their systems. In May 1997, the Office of Management and Budget (OMB) reported that about 21 percent of the mission-critical systems (1,598 of 7,649) for these departments and agencies were Year 2000 compliant.[8] A year later, in May 1998, these departments and agencies reported that 2,914 of the 7,336 mission-critical systems in their current inventories, or about 40 percent, were compliant. Unless progress improves dramatically, a substantial number of mission-critical systems will not be compliant in time.

In addition to slow governmentwide progress in fixing systems, 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. The following are examples of the results of some of our recent reviews.

- Earlier this month, we testified[9] about FAA's progress in implementing a series of recommendations we had made earlier this year to assist FAA in

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

[9]GAO/T-AIMD-98-251, August 6, 1998.

completing overdue awareness and assessment activities.[10] These recommendations included assessing how the major FAA components and the aviation industry would be affected if Year 2000 problems were not corrected in time and completing inventories of all information systems, including data interfaces. Officials at both FAA and the Department of Transportation agreed with these recommendations, and the agency has made progress in implementing them. In our August testimony, we reported[11] 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 must still correct, test, and implement many of its mission-critical systems. It is doubtful that FAA can adequately do all of this in the time remaining. Accordingly, FAA must determine how to ensure continuity of critical operations in the likely event of some systems' failures.

- In October 1997, we reported that while SSA had made significant progress in assessing and renovating mission-critical mainframe software, certain areas of risk in its Year 2000 program remained.[12] Accordingly, we made several recommendations to address these risk areas, which included the Year 2000 compliance of the systems used by the 54 state Disability Determination Services[13] that help administer the disability programs. SSA agreed with these recommendations and, in July 1998, we reported that actions to implement these recommendations had either been taken or were underway.[14] Further, we found that SSA has maintained its place as a federal leader in addressing Year 2000 issues and has made significant progress in achieving systems compliance. However, essential tasks remain. For example, many of the states' Disability Determination Service systems still had to be renovated, tested, and deemed Year 2000 compliant.

[10]Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998) and FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998).

[11]GAO/T-AIMD-98-251, August 6, 1998.

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

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

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

- Our work has shown that much likewise remains to be done in DOD and the military services.[15] For example, our recent 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 have recommended improvements to DOD's and the military services' Year 2000 programs with which they have concurred.

  In addition to these examples, our reviews have shown that many agencies had not adequately acted to establish priorities, solidify data exchange agreements, or develop contingency plans. Likewise, more attention needs to be devoted to (1) ensuring that the government has a complete and accurate picture of Year 2000 progress, (2) setting governmentwide priorities, (3) ensuring that the government's critical core business processes are adequately tested, (4) recruiting and retaining information technology personnel with the appropriate skills for Year 2000-related work, and (5) assessing the nation's Year 2000 risks, including those posed by key economic sectors. I would like to highlight some of these vulnerabilities, and our recommendations made in April 1998 for addressing them.[17]

- First, governmentwide priorities in fixing systems have not yet been established. These 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, 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. 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 has established

[15]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), 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).

[16]GAO/AIMD-98-150, June 30, 1998.

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

48 national priorities covering areas such as national defense, food production, safety, and income security.

- Second, business continuity and contingency planning across the government has been inadequate. In their May 1998 quarterly reports to OMB, only four agencies reported that they had drafted contingency plans for their core business processes. 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 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. Our recently issued guidance aims to help agencies ensure such continuity of operations through contingency planning.[18]
- Third, OMB's assessment of the current status of federal Year 2000 progress is predominantly based on agency reports that have not been consistently reviewed or verified. Without independent reviews, OMB and the President's Council on Year 2000 Conversion have little assurance that they are receiving accurate information. In fact, we have found cases in which agencies' systems compliance status as reported to OMB has been inaccurate. For example, 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 compliant by DOD components.[19] In May 1998, the Department of Agriculture reported (USDA) 15 systems as compliant, even though these were replacement systems that were still under development or were planned for development.[20] (The department plans to remove these systems from compliant status in its next quarterly report.)
- Fourth, end-to-end testing responsibilities have not yet been defined. 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 for their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which

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

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

[20]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).

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 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. So far, 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. We have set forth a structured approach to testing in our recently released exposure draft.[21]

In our April 1998 report on governmentwide Year 2000 progress, we made a number of recommendations to the Chair of the President's Council on Year 2000 Conversion aimed at addressing these problems. These included

- establishing governmentwide priorities and ensuring that agencies set agencywide priorities,
- developing a comprehensive picture of the nation's Year 2000 readiness,
- requiring agencies to develop contingency plans for all critical core business processes,
- requiring agencies to develop an independent verification strategy to involve inspectors general or other independent organizations in reviewing Year 2000 progress, and
- designating lead agencies responsible for ensuring that end-to-end operational testing of processes and supporting systems is performed.

We are encouraged by actions the Council is taking in response to some of our recommendations. For example, OMB and the Chief Information Officers Council adopted our guide providing information on business continuity and contingency planning issues common to most large enterprises as a model for federal agencies.[22] However, as we recently testified before this Subcommittee, some actions have not been initiated—principally with respect to setting national priorities and end-to-end testing.[23]

[21]GAO/AIMD-10.1.21, Exposure Draft, June 1998.

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

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

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—such as benefits payments, transportation, and public safety—that they provide. For example,

- food stamps and other types of payments may not be made or could be made for an incorrect amount,
- 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
- criminal records (i.e., prisoner release or parole eligibility determinations) may be adversely affected by the Year 2000 problem.

Recent surveys of state Year 2000 efforts have indicated that much remains to be completed. For example, a July 1998 survey of state Year 2000 readiness conducted by the National Association of State Information Resource Executives, Inc., found that only about one-third of the states reported that 50 percent or more of their critical systems[24] had been completely assessed, remediated, and tested.

In a June 1998 survey conducted by USDA's Food and Nutrition Service, only 3 and 14 states,[25] respectively, reported that the software, hardware, and telecommunications that support the Food Stamp Program, and the Women, Infants, and Children program, were Year 2000 compliant. Although all but one of the states reported that they would be Year 2000 compliant by January 1, 2000, many of the states reported that their systems are not due to be compliant until after March 1999 (the federal government's Year 2000 implementation goal). Indeed, 4 and 5 states, respectively, reported that the software, hardware, and telecommunications supporting the Food Stamp Program, and the Women, Infants, and Children program would not be Year 2000 compliant until the last quarter of calendar year 1999, which puts them at high risk of failure due to the need for extensive testing.

To effectively manage their Year 2000 projects and mitigate their Year 2000 risks, state and local governments must perform the same types of activities as the federal government. Such activities would include priority

[24]Critical systems were defined as "systems that effect public safety, public health, and financial and personnel aspects of government services."

[25]The Food and Nutrition Service included the District of Columbia, Guam, Puerto Rico, and the Virgin Islands in its survey. The Food and Nutrition Service did not verify the information provided by the states.

setting, progress reporting, and contingency planning. For example, according to the Texas Year 2000 Project Office's Internet World Wide Web site, the project office has set up a mechanism for state agencies and universities to use to report on their progress and actively monitors the progress of the state's highest priority agencies (those that affect public health and safety and the economic well-being of the State of Texas).

In May 1998, the Texas project office stated that it was "cautiously optimistic that most Mission Critical functions will not be disrupted by the Year 2000 problem." However, the project office added that "this does not mean that agencies and universities will complete their projects on time and on budget." The project office reported[26] that 3 priority agencies were "on target,"[27] 12 priority agencies were in the "watch" category,[28] and 4 priority agencies "at risk."[29]

The Texas Year 2000 Project Office has also issued a business contingency planning guide to its agencies and universities, and directed that agencies and universities meet certain milestones related to business contingency planning. For example, by the end of this month, agencies and universities are to begin the contingency planning process and develop Year 2000 contingency planning assessments that would identify areas that may be at risk. In addition, by January 31, 1999, agencies and universities are to develop detailed business contingency plans.

Texas' Office of the State Auditor recently reported[30] on the state's efforts to remediate its embedded systems,[31] which, if not corrected, could

[26]Based on March 1998 data.

[27]According to the Texas Year 2000 Project Office, "on target" means that the project office has confidence that Year 2000 remediation is complete or on schedule for completion well before problems would occur or that adequate planning is in place to ensure that the state will not be affected by any failures.

[28]According to the Texas Year 2000 Project Office, "watch" means that Year 2000 remediation was not complete and the schedule for remediation is not robust or that certain risks must be managed successfully in order to complete the project on time. Agencies or universities may also be classified in the "watch" category because of the importance of their Year 2000 projects to the overall operation of Texas' state government.

[29]According to the Texas Year 2000 Project Office, the "at risk" agencies are similar to the "watch" agencies but are a greater risk to manage and, because of their special importance to the people of Texas, the consequences of failure are especially acute.

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

[31]Embedded systems are special-purpose computers built into other devices. They are used in, for example, security systems, prison control units, and certain medical equipment.

disrupt critical state services. The State Auditor found that many state entities had not finished their embedded systems inventories and, therefore, it is not likely that they will complete their embedded systems repairs before the year 2000. In addition, the report noted that (1) many entities lacked contingency plans in case their embedded systems fail, (2) several entities cited a lack of funds as a barrier to embedded systems repair efforts, and (3) no entity is responsible for coordinating and reporting on statewide embedded systems repair efforts. To address these concerns, the Office of the State Auditor also made recommendations, such as the Texas Year 2000 Project Office including embedded systems in its Year 2000 contingency plan requirements.

Audits of other states by their audit organizations have identified other significant Year 2000 concerns. For example, (1) Illinois' Office of the Auditor General reported that significant future efforts were needed to ensure that the year 2000 would not adversely affect state government operations,[32] (2) Vermont's Office of Auditor of Accounts reported that the state faces the risk that critical portions of its Year 2000 compliance efforts could fail,[33] and (3) Florida's Auditor General has issued several reports detailing the need for additional Year 2000 planning at various district school boards and community colleges.[34] 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.

Federal/State Data Exchanges Critical to Delivery of Services

To fully address the Year 2000 risks that states and the federal government face, data exchanges must also be confronted—a monumental issue. As computers play an ever-increasing role in our society, exchanging data electronically has become a common method of transferring information among federal, state, and local governments. For example, SSA exchanges data files with the states to determine the eligibility of disabled persons for disability benefits. In another example, the National Highway Traffic Safety Administration provides states with information needed for driver registrations. As computer systems are converted to process Year 2000

[32]Bureau of Communications and Computer Services Third Party Review (July 1, 1998).

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

[34]Examples of these reports include, Report on Audit of the Alachua County District School Board For The Fiscal Year Ended June 30, 1997 (Report No. 13219, April 21, 1998) and Operational Audit of the District Board of Trustees Broward Community College For The Period July 1, 1996 through June 30, 1997 (Report No. 13222, April 30, 1998). The Year 2000 work for these reports was performed in early 1998.

dates, the associated data exchanges must also be made Year 2000 compliant. If the data exchanges are not Year 2000 compliant, data will not be exchanged or invalid data could cause the receiving computer systems to malfunction or produce inaccurate computations.

Our recent report[35] on actions that have been taken to address Year 2000 issues for electronic data exchanges[36] revealed that federal agencies and the states use thousands of such exchanges to communicate with each other and other entities. For example, federal agencies reported that their mission-critical systems have almost 500,000 data exchanges with other federal agencies, states, local governments, and the private sector.

To successfully remediate their data exchanges, federal agencies and the states must (1) assess information systems to identify data exchanges that are not Year 2000 compliant, (2) contact exchange partners and reach agreement on the date format to be used in the exchange, (3) determine if data bridges and filters are needed and, if so, reach agreement on their development, (4) develop and test such bridges and filters,[37] (5) test and implement new exchange formats, and (6) develop contingency plans and procedures for data exchanges.

At the time of our review, much work remained to ensure that federal and state data exchanges will be Year 2000 compliant. About half of the federal agencies reported during the first quarter of 1998 that they had not yet finished assessing their data exchanges. Moreover, almost half of the federal agencies reported that they had reached agreements on 10 percent or fewer of their exchanges,[38] few federal agencies reported having installed bridges or filters, and only 38 percent of the agencies reported that they had developed contingency plans for data exchanges.

Further, the status of the data exchange efforts of 15 of the 39 state-level organizations that responded to our survey was not discernable because they were not able to provide us with information on their total number of

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

[36]To perform this review, we developed and sent a data collection instrument to survey 42 federal departments, all states, the District of Columbia, and Puerto Rico.

[37]A bridge is used to convert incoming two-digit years to four-digit years or to convert outgoing 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.

[38]This does not include the status of agreements reported by the Federal Reserve. The Federal Reserve controls the data exchange software used by its partners and does not need to reach agreement with exchange partners on formats.

exchanges and the number assessed. Of the 24 state-level organizations that provided actual or estimated data, they reported, on average, that 47 percent of the exchanges had not been assessed. In addition, similar to the federal agencies, state-level organizations reported having made limited progress in reaching agreements with exchange partners, installing bridges and filters, and developing contingency plans. However, we could draw only limited conclusions on the status of the states actions because data were provided on only a small portion of states' data exchanges.

To strengthen efforts to address data exchanges, we made several recommendations to OMB. In response, OMB agreed that it needed to increase its efforts in this area. For example, OMB noted that federal agencies had provided the General Services Administration with a list of their data exchanges with the states. In addition, as a result of an agreement reached at an April 1998 federal/state data exchange meeting,[39] the states were supposed to verify the accuracy of these initial lists by June 1, 1998.[40] OMB also noted that the General Services Administration is planning to collect and post information on its Internet World Wide Web site on the progress of federal agencies and states in implementing Year 2000 compliant data exchanges.

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

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

[39]Initial agreements between the federal government and the states on steps to address Year 2000 data exchange issues were reached at an October 1997 state/federal summit, sponsored by the federal Chief Information Officer Council and National Association of State Information Resource Executives, Inc., and hosted by the Commonwealth of Pennsylvania.

[40]According to the National Association of State Information Resource Executives, Inc., as of early August 1998, 16 states had completed the verification of their federal/state data exchanges and an additional 9 states had completed 80 percent of the verification.

GAO Reports and Testimony Addressing the Year 2000 Crisis

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: A Testing Guide (GAO/AIMD-10.1.21, Exposure Draft, June 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 (GAO/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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested