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
1 p.m.
Monday,
June 22, 1998

YEAR 2000 COMPUTING CRISIS

Testing and Other Challenges Confronting Federal Agencies

Statement of Dr. Rona B. Stillman
Chief Scientist for Computers and Telecommunications
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the Year 2000 problem. As you know, the federal government is extremely vulnerable to Year 2000 problems due to its widespread dependence on computer systems to process financial transactions, deliver vital public services, maintain national security, and carry out its operations. This challenge is made more difficult by the age and poor documentation of some of the government's existing systems and its lackluster track record in modernizing systems to deliver expected improvements and meet promised deadlines. Today, I will briefly discuss the Year 2000 risks facing the government; highlight our major concerns with the government's progress in fixing its systems; and introduce our guidance on Year 2000 testing, which is designed to assist agencies in the most extensive and expensive part of remediation.

Risk of Year 2000 Disruption to Government Services Is High

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.

To complicate matters, agencies must also consider the computer systems belonging to federal, state, and local governments; the private sector; foreign countries; and international organizations that interface with their systems. For example, agencies that administer key federal benefits payment programs, such as the Department of Veterans Affairs, exchange data with the Department of the Treasury, which, in turn, interfaces with various financial institutions to ensure that benefits checks are issued. Department of Defense (DOD) systems interface with thousands of systems belonging to foreign military sales customers, private contractors, other federal agencies, and international entities such as the North Atlantic Treaty Organization. Taxpayers can pay their taxes through data exchanges between the taxpayer, financial institutions, the Federal Reserve System, and the Department of the Treasury's Financial Management Service and the Internal Revenue Service. Because of these and thousands of other interdependencies, government systems are also vulnerable to failure caused by incorrectly formatted data provided by other systems that are noncompliant.

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. Seamless connectivity among a wide range of networks and carriers is essential nationally and internationally and a Year 2000-induced telecommunications failure could cause major disruptions.

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. For example:

- flights could be grounded or delayed and airline safety could be degraded;
- the military services could find it extremely difficult to efficiently and effectively equip and sustain their forces around the world;
- Internal Revenue Service tax systems could be unable to process returns, thereby jeopardizing revenue collection and delaying refunds;
- the Social Security Administration process to provide benefits to disabled persons could be disrupted; and
- payments to veterans with service-connected disabilities could be erroneous or severely delayed.

Key Year 2000 Issues Are Not Being Adequately Addressed

Because of the urgent nature of the Year 2000 problem and the potentially devastating impact it can have on critical government operations, we designated the problem as a high-risk area for the federal government in February 1997.[1] Since that time, we have issued over 40 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[2] We

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

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

have also issued guidance to help organizations successfully address the issue.[3]

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.[4] 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 on time.

In addition to slow progress in fixing systems, many agencies were not adequately acting on critical steps to establish priorities, solidify data exchange agreements, and develop contingency plans. Likewise, more attention needs to be devoted to (1) ensuring the government has a complete and accurate picture of Year 2000 progress, (2) setting national 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.[5]

- First, governmentwide priorities in fixing systems have yet to be established. There has not been a concerted effort to set governmentwide priorities 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. Furthermore, while individual agencies have been identifying mission-critical systems, this has not always been done based on a

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

[4]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.

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

determination of the agency's most critical operations. For example, as noted by the Defense Science Board, Defense has no means of distinguishing between the priority of a video-conferencing system and a logistics system, both of which were identified as mission-critical. 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.

- Second, 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.
- 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 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.[6] 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 to be developed.[7] (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

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

[7]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).

for their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, work as intended in an operational environment. 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.

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

- establishing governmentwide priorities and ensuring that agencies set their own 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 inspector general or other independent organizations in reviewing Year 2000 progress, and
- designating lead agencies responsible for ensuring 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 draft guide providing information on business continuity and contingency planning issues common to most large enterprises as a model for federal agencies.[8] However, as we recently testified before this Subcommittee, some actions have not been initiated—principally with respect to setting national priorities, independent verification, and end-to-end testing.

[8]GAO/AIMD-10.1.19, Exposure Draft, March 1998.

GAO Guidance on Year 2000 Testing

One of the more alarming problems we have come across in our Year 2000 reviews is that some agencies are not adequately prepared for testing their systems for Year 2000 compliance. For example, in April 1998, we reported that DOD did not have a testing strategy that specifies uniform criteria and processes that its components should use in testing their systems. The Army, Navy, and Air Force had not assessed their test needs or test facility requirements.[9] In May 1998, we reported that the Department of Agriculture's Chief Information Officer had not provided test guidance to the department's component agencies, and 8 of 10 component agencies included in our review lacked testing strategies.[10]

The fact that these agencies are not prepared now for effective testing raises serious concern. Complete and thorough Year 2000 testing is essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core business operations after the millennium. Moreover, since the Year 2000 computing problem is so pervasive, potentially affecting an organization's systems software, applications software, databases, hardware, firmware and embedded processors, telecommunications, and external interfaces, the requisite testing is extensive and expensive. Leading organizations estimate that testing will require at least 50 percent of an entity's total Year 2000 program time.

To address this problem, we are issuing today a new installment of our Year 2000 guidance which addresses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.[11] The guide describes a step-by-step framework for managing, and a checklist for assessing, all Year 2000 testing activities, including those activities associated with computer systems or system components (such as embedded processors) that are vendor supported. This disciplined approach and the prescribed levels of testing activities are hallmarks of mature software and system development/acquisition and maintenance processes.

The guide describes the five levels of Year 2000 testing activities. The first level establishes the organization infrastructure key processes needed to guide, support, and manage the next four levels of testing activities. For example, it addresses defining and assigning Year 2000 test management

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

[10]GAO/T-AIMD-98-167, May 14, 1998.

[11]Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, Exposure Draft, June 1998).

authority and responsibility, defining criteria for certifying a system as compliant, identifying and allocating resources, establishing schedules, and securing test facilities. The next four levels provide key processes for effectively designing, conducting, and reporting on tests of incrementally larger system components: software unit/module tests, software integration tests, system acceptance tests, and end-to-end tests. The processes focus on testing of software and system components that the organization is directly responsible for developing, acquiring, or maintaining. Key processes, however, are also defined to address organizational responsibilities relative to testing of vendor-supported and commercial, off-the-shelf (COTS) products and components (including hardware, systems software, embedded processors, telecommunications, and COTS applications).

The test model builds upon and complements the five-phase conversion model described in our Year 2000 readiness guide. The five levels of test activities span all phases of our Year 2000 conversion model, with the preponderance of test activities occurring in the conversion model's renovation and validation phases.

Finally, the guide incorporates guidance and recommendations of standards bodies, such as the National Institute of Standards and Technology and the Institute of Electrical and Electronic Engineers on Year 2000 testing practices and draws on the work of leading information technology organizations including the Software Engineering Institute, Software Quality Engineering, Software Productivity Consortium, and the United Kingdom's Central Computer and Telecommunications Agency.

In conclusion, if effectively implemented, our guide should help federal agencies successfully negotiate the complexities involved with the Year 2000 testing process. However, the success of the government's Year 2000 remediation efforts ultimately hinges on setting governmentwide priorities; ensuring that agencies set priorities and develop contingency plans consistent with these priorities; developing an accurate picture of remediation progress; designating lead agencies for end-to-end testing efforts; and addressing other critical issues, such as recruiting and retaining qualified information technology personnel.

Mr. Chairman, this concludes my statement. Mr. Joel Willemssen, GAO's Issue Area Director for Civil Agencies Information Systems and our focal

point for Year 2000 work, has accompanied me today. We will be happy to answer any questions you or Members of the Subcommittee may have.

List of GAO Products That Address the Year 2000 Problem

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).

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

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

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

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

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

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

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

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

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

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