United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
9:30 a.m.
Wednesday,
March 18, 1998

# YEAR 2000 COMPUTING CRISIS

# Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions

Statement of Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

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

We are pleased to be here today to discuss the Year 2000 computing crisis. 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] As a result, the upcoming change of century is a sweeping and urgent challenge for public and private-sector organizations.[2]

For this reason, we designated the Year 2000 computing problem as a high-risk area[3] for the federal government and published guidance[4] to help organizations successfully address the issue. During the past year, we have issued over two dozen reports detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[5]

While some progress has been made in addressing the federal government's Year 2000 readiness, serious vulnerabilities remain. Many agencies are behind schedule. At the current pace, it is clear that not all mission critical systems will be fixed in time. Much more action is needed to ensure that federal agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences. Vital economic sectors of the nation are also vulnerable. These include state and local governments; telecommunications; banking and finance; health, safety, and emergency services; transportation; utilities; and manufacturing and small business.

While actions by government and industry are underway throughout the nation, the recent creation of the President's Council on Year 2000 Conversion represents a much needed approach to orchestrate the

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

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

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

[4] Our enterprise readiness guide—Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)—offers a structured, step-by-step approach for reviewing the adequacy of agency planning and management of a Year 2000 program. This guide was released to the public as an exposure draft in February 1997 and issued in September 1997.

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

leadership and public/private partnerships essential to confronting the unprecedented challenges posed by the Year 2000 crisis. Our testimony today outlines Year 2000 risks and presents actions that should be taken by the President's Council. We have provided for comment a draft report on these issues to the Chairman of the President's Council on Year 2000 Conversion and the Office of Management and Budget (OMB) and expect to issue it soon.

## Reliance on Computers and Interdependencies Among Sectors Create Risk of Service Disruption

The public faces a risk that critical services could be severely disrupted by the Year 2000 computing crisis. Financial transactions could be delayed, airline flights grounded, and national defense affected. The many interdependencies that exist among governments and within key economic sectors could cause a single failure to have adverse repercussions. While managers in the government and the private sector are taking many actions to mitigate these risks, a significant amount of work remains, and time frames are unrelenting.

### Risk of Disruption to Government Services Is High

The federal government is extremely vulnerable to the Year 2000 issue due to its widespread dependence on computer systems to process financial transactions, deliver vital public services, and carry out its operations. This challenge is made more difficult by the age and poor documentation of the government's existing systems and its lackluster track record in modernizing systems to deliver expected improvements and meet promised deadlines.

Unless this issue is successfully addressed, serious consequences could ensue. For example:

- 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]
- Payments to veterans with service-connected disabilities could be severely delayed if the system that issues them either halts or produces checks so erroneous that it must be shut down and checks processed manually.
- The military services could find it extremely difficult to efficiently and effectively equip and sustain their forces around the world.
- Federal systems used to track student loans could produce erroneous information on loan status, such as indicating that a paid loan was in default.

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

- 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 if interfaces with state systems fail.

In addition, the year 2000 also could cause problems for the many facilities used by the federal government that were built or renovated within the last 20 years that contain embedded computer systems[7] to control, monitor, or assist in operations. For example, heating and air conditioning units could stop functioning properly and card-entry security systems could cease to operate.

Year 2000-related problems have already been identified. For example, an automated Defense Logistics Agency system erroneously deactivated 90,000 inventoried items as the result of an incorrect date calculation. According to the agency, if the problem had not been corrected (which took 400 work hours), the impact would have seriously hampered its mission to deliver materiel in a timely manner.[8] In another case, the Department of Defense's Global Command Control System, which is used to generate a common operating picture of the battlefield for planning, executing, and managing military operations, failed testing when the date was rolled over to the year 2000.

Our reviews of federal agency Year 2000 programs 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 remain and a great deal more work is needed. Our reports contained numerous recommendations, which the agencies have almost universally agreed to implement. Among them were the need to complete inventories of systems, document data exchange agreements, and develop contingency plans.

Audit offices of some states also have identified significant Year 2000 concerns. Risks include the potential that systems supporting benefit programs, motor vehicle records, and criminal records (i.e., prisoner release or parole eligibility determinations) may be adversely affected. These audit offices have made recommendations including the need for increased oversight, Year 2000 project plans, contingency plans, and personnel recruitment and retention strategies.

[7] Embedded systems are special-purpose computers built into other devices.

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

Data exchanges between the federal government and the states are also critical to ensuring that billions of dollars of benefits payments are made to millions of recipients. Consequently, in October 1997 the Commonwealth of Pennsylvania hosted the first State/Federal Chief Information Officer (CIO) Summit. Participants agreed to (1) use a four-digit contiguous computer standard for data exchanges, (2) establish a national policy group, and (3) create a joint state/federal working group.

## Key Economic Sectors at Risk of Year 2000 Failures

America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. Key economic sectors that could be seriously affected if their systems are not Year 2000 compliant are information and telecommunications; banking and finance; health, safety, and emergency services; transportation; utilities; and manufacturing and small business.[9] The information and telecommunications infrastructure is especially important because it (1) enables the electronic transfer of funds, (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. Illustrations of Year 2000 risks follow.

- 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. Moreover, the Chair of the Federal Financial Institutions Examination Council, a U.S. interagency council composed of federal bank, credit union, and thrift institution regulators, stated that banking is one of America's most information-intensive businesses and that any malfunctions caused by the century date change could affect a bank's ability to meet its obligations. He also stated that of equal concern are problems that customers may experience that could prevent them from meeting their obligations to banks and that these problems, if not addressed, could have repercussions throughout the nation's economy.
- According to the International Organization of Securities Commissions, the Year 2000 presents a serious challenge to the world's financial markets. Because they are highly interconnected, a disruption in one segment can spread quickly to others.

[9] These sectors are compatible with the critical infrastructures identified by the President's Commission on Critical Infrastructure Protection. The Commission deemed these infrastructures so vital that their destruction or incapacity would have a debilitating impact on our defense and economic security.

- FAA recently met with representatives of airlines, aircraft manufacturers, airports, fuel suppliers, telecommunications providers, and industry associations to discuss the Year 2000 issue. Participants raised the concern that their own Year 2000 compliance would be irrelevant if FAA were not compliant because of the many system interdependencies. Representatives went on to say that unless FAA were substantially Year 2000 compliant on January 1, 2000, flights would not get off the ground and that extended delays would be an economic disaster.
- Another risk associated with the transportation sector was described by the Federal Highway Administration, which stated that highway safety could be severely compromised because of potential Year 2000 problems in operational transportation systems. For example, date-dependent signal timing patterns could be incorrectly implemented at highway intersections if traffic signal systems run by state and local governments do not process four-digit years correctly.
- One risk associated with the utility sector is the potential loss of electrical power. For example, Nuclear Regulatory Commission staff believe that safety-related safe shutdown systems will function but that a worst-case scenario could occur in which Year 2000 failures in several nonsafety-related systems could cause a plant to shut down, resulting in the loss of off-site power and complications in tracking post-shutdown plant status and recovery.
- With respect to the health, safety, and emergency services sector, according to the Department of Health and Human Services, the Year 2000 issue holds serious implications for the nation's health care providers and researchers. 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. In addition, according to the Gartner Group, health care is substantially behind other industries in Year 2000 compliance, and it predicts that at least 10 percent of mission-critical systems in this industry will fail because of noncompliance.[10]

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. In September 1997, the Gartner Group surveyed 2,400 companies in 17

[10] Healthcare Is Far Behind In Year 2000 Compliance (Gartner Group, Document #IGG-020498-02, February 4, 1998).

countries and concluded that “[t]hirty percent of all companies have not started dealing with the year 2000 problem.”[11]

Although there are many national and international risks related to the year 2000, our limited review of these key sectors found a number of private-sector organizations that have raised awareness and provided advice. For example:

- The Securities Industry Association established a Year 2000 committee in 1995 to promote awareness and since then has established other committees to address key issues, such as testing.
- The Electric Power Research Institute sponsored a conference in 1997 with utility professionals to explore the Year 2000 issue in embedded systems.
- Representatives of several oil and gas companies formed a Year 2000 energy industry group, which meets regularly to discuss the problem.
- The International Air Transport Association organized seminars and briefings for many segments of the airline industry.

In addition, information technology industry associations, such as the Information Technology Association of America, have published newsletters, issued guidance, and held seminars to focus information technology users on the Year 2000 problem.

## Additional Actions Can Be Taken to Reduce Year 2000 Risks

As 2000 approaches and the scope of the problems has become clearer, the federal government’s actions have intensified, at the urging of the Congress and others. The amount of attention devoted to this issue has increased in the last year, culminating with the issuance of a February 4, 1998, executive order establishing the President’s Council on Year 2000 Conversion. The Council Chair is to oversee federal agency Year 2000 efforts as well as act as spokesman in national and international forums, coordinate with state and local governments, promote appropriate federal roles with respect to private-sector activities, and report to the President on a quarterly basis.

This increased attention could help minimize the disruption to the nation as the millennium approaches. In particular, the President’s Council on Year 2000 Conversion can initiate additional actions needed to mitigate risks and uncertainties. These include ensuring that the government’s

[11] Year 2000-World Status (Gartner Group, Document #M-100-037, November 25, 1997).

highest priority systems are corrected and that contingency plans are developed across government.

## Setting Priorities Is Critical

Agencies have taken longer to complete the awareness and assessment phases of their Year 2000 programs than is recommended. This leaves less time for critical renovation, validation, and implementation phases. For example, the Air Force has used over 45 percent of its available time completing the awareness and assessment phases, while the Gartner Group recommends that no more than about a quarter of an organization's Year 2000 effort should be spent on these phases.

Consequently, priority-setting is essential. According to OMB's latest report, as of February 15, 1998, only about 35 percent of federal agencies' mission-critical systems were considered to be Year 2000 compliant. This leaves over 3,500 mission-critical systems, as well as thousands of nonmission-critical systems, still to be repaired, and over 1,100 systems to be replaced. It is unlikely that agencies can complete this vast amount of work in time. Accordingly, it is critical that the executive branch identify those systems that are of the highest priority. These include those that, if not corrected, could most seriously threaten health and safety, the financial well-being of American citizens, national security, or the economy.

Agencies must also ensure that their mission-critical systems can properly exchange data with other systems and are protected from errors that can be introduced by external systems. For example, agencies that administer key federal benefits payment programs, such as the Department of Veterans Affairs, must exchange data with the Department of the Treasury, which, in turn, interfaces with financial institutions, to ensure that beneficiary checks are issued. As a result, completing end-to-end testing for mission-critical systems is essential.

## Reporting on Agency Progress Needs to Be Improved

OMB's reports on agency progress do not fully and accurately reflect the federal government's progress toward achieving Year 2000 compliance because not all agencies are required to report and OMB's reporting requirements are incomplete. For example:

- OMB had not, until recently, required independent agencies to submit quarterly reports. Accordingly, the status of these agencies' Year 2000 programs has not been monitored centrally. On March 9, 1998, OMB asked

31 independent agencies, including the Securities and Exchange Commission and the Pension Benefit Guaranty Corporation, to report on their progress in fixing the Year 2000 problem by April 30, 1998. OMB plans to include a summary of those responses in its next quarterly report to the Congress. However, unlike its quarterly reporting requirement for the major departments and agencies, OMB does not plan to request the independent agencies to report again until next year. Since the independent agencies will not be reporting again until April 1999, it will be difficult for OMB to be in position to address any major problems.

- Agencies are required to report their progress in repairing noncompliant systems but are not required to report on their progress in implementing systems to replace noncompliant systems, unless the replacement effort is behind schedule by 2 months or more. Because federal agencies have a poor history of delivering new system capabilities on time, it is essential to know agencies' progress in implementing replacement systems.
- OMB's guidance does not specify what steps must be taken to complete each phase of a Year 2000 program (i.e., assessment, renovation, validation, and implementation). Without such guidance, agencies may report that they have completed a phase when they have not. Our enterprise guide provides information on the key tasks that should be performed within each phase.[12]

Mr. Chairman, in your December 1997 letter to OMB, you expressed similar concerns that OMB reports be more comprehensive and reliable.

## Contingency Plans Imperative

In January 1998, OMB asked agencies to describe their contingency planning activities in their February 1998 quarterly reports. These instructions stated that contingency plans should be established for mission-critical systems that are not expected to be implemented by March 1999, or for mission-critical systems that have been reported as 2 months or more behind schedule. Accordingly, in their February 1998 quarterly reports, several agencies reported that they planned to develop contingency plans only if they fall behind schedule in completing their Year 2000 fixes.

Agencies that develop contingency plans only for systems currently behind schedule, however, are not addressing the need to ensure the continuity of a minimal level of core business operations in the event of unforeseen failures. As a result, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and

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

test effective contingency plans. Contingency plans should be formulated to respond to two types of failures: those that can be predicted (e.g., system renovations that are already far behind schedule) and those that are unforeseen (e.g., a system that fails despite having been certified as Year 2000 compliant or a system that cannot be corrected by January 1, 2000, despite appearing to be on schedule today).

Moreover, contingency plans that focus only on agency systems are inadequate. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure. One weak link anywhere in the chain of critical dependencies can cause major disruptions. 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.

In its latest governmentwide Year 2000 progress report, issued March 10, 1998, OMB clarified its contingency plan instructions.[13] OMB stated that contingency plans should be developed for all core business functions. Today, we are issuing an exposure draft of a guide to help agencies ensure the continuity of operations through contingency planning.[14] The CIO Council worked with us in developing this guide and intends to adopt it for federal agency use.

## Independent Verification of Progress Needed

OMB's assessment of the current status of federal Year 2000 progress has been predominantly based on agency reports that have not been consistently verified or independently reviewed. Without such independent reviews, OMB and others, such as the President's Council on Year 2000 Conversion, have no assurance that they are receiving accurate information. OMB has acknowledged the need for independent verification and asked agencies to report on such activities in their February 1998 quarterly reports. While this has helped provide assurance that some verification is taking place through internal checks, reviews by Inspectors General, or contractors, the full scope of verification activities required by OMB has not been articulated.

It is important that the executive branch set standards for the types of reviews that are needed to provide assurance regarding the agencies' Year

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

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

2000 actions. Such standards could encompass independent assessments of (1) whether the agency has developed and is implementing a comprehensive and effective Year 2000 program, (2) the accuracy and completeness of the agency's quarterly report to OMB, including verification of the status of systems reported as compliant, (3) whether the agency has a reasonable and comprehensive testing approach, and (4) the completeness and reasonableness of the agency's business continuity and contingency planning.

## Ability to Address Governmentwide Issues Could Be Strengthened

The CIO Council's Subcommittee on the Year 2000 has been useful in addressing governmentwide issues. For example, the Year 2000 Subcommittee worked with the Federal Acquisition Regulation Council and industry to develop a rule that (1) establishes a single definition of Year 2000 compliance in executive branch procurement and (2) generally requires agencies to acquire only Year-2000 compliant products and services or products and services that can be made Year 2000 compliant. The subcommittee has also established subgroups on (1) best practices, (2) state issues and data exchanges, (3) industry issues, (4) telecommunications, (5) buildings, (6) biomedical and laboratory equipment, (7) General Services Administration support and commercial off-the-shelf products, and (8) international issues.

The subcommittee's effectiveness could be further enhanced. For example, currently agencies are not required to participate in the Year 2000 subcommittee. Without such full participation, it is less likely that appropriate governmentwide solutions can be implemented. Further, while the subcommittee's subgroups are currently working on plans, they have not yet published these with associated milestones. It is important that this be done and publicized quickly so that agencies can use this information in their Year 2000 programs. It is equally important that implementation of agency activities resulting from these plans be monitored closely and that the subgroups' decisions be enforced.

Another governmentwide issue that needs to be addressed is the availability of information technology personnel. In their February 1998 quarterly reports, several agencies reported that they or their contractors had problems obtaining and/or retaining information technology personnel. Currently, no governmentwide strategy exists to address recruiting and retaining information technology personnel with the appropriate skills for Year 2000-related work. To date, the CIO Council has not addressed this issue although it is considering asking the Office of

Personnel Management to review the possibility of obtaining waivers to rehire retired federal personnel.

## Success of the New Presidential Council Is Critical

Given the sweeping ramifications of the Year 2000 issue, other countries have set up mechanisms to solve the Year 2000 problem on a nationwide basis. Several countries, such as the United Kingdom, Canada, and Australia, have appointed central organizations to coordinate and oversee their governments' responses to the Year 2000 crisis. In the case of the United Kingdom, for example, a ministerial group is being established, under the leadership of the President of the Board of Trade, to tackle the Year 2000 problem across the public and private sectors.

These countries have also established public/private forums to address the Year 2000 problem. For example, in September 1997, Canada's Minister of Industry established a government/industry Year 2000 task force of representatives from banking, insurance, transportation, manufacturing, telecommunications, information technology, small and medium-sized businesses, agriculture, and the retail and service sectors. The Canadian Chief Information Officer is an ex-officio member of the task force. It has been charged with providing (1) an assessment of the nature and scope of the Year 2000 problem, (2) the state of industry preparedness, and (3) leadership and advice on how risks could be reduced. This task force issued a report in February 1998 with 18 recommendations that are intended to promote public/private-sector cooperation and prompt remedial action.

In the United States, the President's recent executive order could serve as the linchpin that bridges the nation's and the federal government's various Year 2000 initiatives. While the Year 2000 problem could have serious consequences, there is no comprehensive picture of the nation's readiness. As one of its first tasks, the President's Council on Year 2000 Conversion could formulate such a comprehensive picture in partnership with the private sector and state and local governments.

Many organizational and managerial models exist that the Conversion Council could use to build effective partnerships to solve the nation's Year 2000 problem. Because of the need to move swiftly, one viable alternative would be to consider using the sector-based approach recommended recently by the President's Commission on Critical Infrastructure Protection as a starting point.

This approach could involve federal agency focal points working with sector infrastructure coordinators. These coordinators would be created or selected from existing associations and would facilitate sharing information among providers and the government. Using this model, the President's Council on Year 2000 Conversion could establish public/private partnership forums composed of representatives of each major sector that, in turn, could rely on task forces organized along economic-sector lines. Such groups would help (1) gauge the nation's preparedness for the year 2000, (2) periodically report on the status and remaining actions of each sector's Year 2000 remediation efforts, and (3) ensure the development of contingency plans to ensure the continuing delivery of critical public and private services.

In conclusion, while the Year 2000 problem has the potential to cause serious disruption to the nation, these risks can be mitigated and disruptions minimized with proper attention and management. Continued congressional oversight through hearings such as this and those that have been held by other committees in both the House and the Senate can help ensure that the Year 2000 problem is given the attention that it deserves and that appropriate actions are taken to address this crisis.

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

# GAO Reports and Testimony Addressing the Year 2000 Crisis

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 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 Computers Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997).

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

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

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

PRINTED ON ♻ RECYCLED PAPER