

GAO

Testimony

Before the Subcommittee on Oversight,
Committee on Ways and Means,
House of Representatives

For Release on Delivery
Expected at
3 p.m.
Tuesday,
June 16, 1998

YEAR 2000 COMPUTING CRISIS

Telecommunications Readiness Critical, Yet Overall Status Largely Unknown

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



Madam Chairwoman and Members of the Subcommittee:

We are pleased to join you today to discuss the computing crisis posed by the upcoming change of century, and its implications in one critical area: telecommunications. As you know, the year 2000 presents a particularly sweeping and urgent challenge for entities in this country.¹ For this reason, in February 1997 we designated the Year 2000 problem as a high-risk area² for the federal government, and have published guidance³ to help organizations successfully address the issue. Since that time we have issued over 45 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 compliance of a wide range of federal agency systems.⁴ The common theme has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness, and that much more action is needed to ensure that agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences.

We have made many recommendations to the executive branch to reduce the risk of Year 2000-induced disruptions of critical services. Among these, we recommended that the Chair of the President's Council on Year 2000 Conversion develop a comprehensive picture of the nation's Year 2000 readiness. This effort would include identifying and assessing the risk of the nation's key economic sectors, including those posed by telecommunications.

The readiness of the telecommunications sector is one of the most crucial concerns. No one—large corporation, small business, government agency, family, or individual—is immune from the potential disruption of vital telecommunications services. The United States, with almost half of the world's computer capacity and 60 percent of Internet assets, is the world's most advanced—and most dependent—producer and user of information

¹For 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.

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

³Year 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, March 1998 [exposure draft]), which describes the tasks needed to ensure the continuity of agency operations.

⁴A listing of our publications is included as an attachment to this statement.

and telecommunications technologies.⁵ In particular, such technologies have helped fuel the growth of the U.S. economy and have enabled major improvements in the nation's infrastructure. As a result, telecommunications service providers and their public- and private-sector customers have a lot at stake; the potential losses and disruptions that could accrue from noncompliant telecommunications systems could be staggering.

My testimony today will (1) describe our nation's telecommunications infrastructure, (2) discuss the risks we face if critical components of that infrastructure are not Year 2000 compliant by the turn of the century, (3) describe federal government actions relating to national, international, and governmental telecommunications infrastructure, and (4) present issues that must be addressed.

The Telecommunications Infrastructure

The telecommunications infrastructure comprises the public telecommunications network; the Internet; and the millions of computer systems for government, defense, commercial, and personal use. The public network includes a complex web of interconnected networks operated by local and long-distance carriers, cellular networks, and satellite services. The Internet is a global network of networks interconnected by routers⁶ using a common set of protocols.⁷ Significant portions of the Internet rely on services provided by the public telecommunications networks.

The rich array of reliable telecommunications services is made possible by a complex web of highly interconnected networks supported by switches⁸ and other telecommunications devices. Along with national and local carriers and service providers, other important links in the chain are the equipment manufacturers and suppliers and customers, some of whom have specific telecommunications devices installed on their premises,

⁵Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

⁶Routers are devices that direct messages. Routers receive packets of information from computers or other routers on the network; they then send these packets to their destinations based on "addresses" at the beginning of the packets and a road map of the other computers and peripherals on the network.

⁷Protocols are a set of procedures for establishing and controlling data transmission.

⁸Switches are electronic or mechanical devices that allow connections to be established as necessary and terminated when there is no longer a session to support.

such as private branch exchanges (PBX),⁹ and voice mail systems. The key is connectivity: all of the pieces must work together.

Services Vital to the Nation Depend Upon Reliable Telecommunications

Telecommunications are critical to the operations of nearly every public- and private-sector organization. All other major sectors rely on it: banking and finance; health, safety, and emergency services; transportation; utilities; and manufacturing and small business. For example, 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.

The federal government depends on the telecommunications infrastructure to deliver a wide range of services. Many agencies, including those in the Department of the Treasury and Department of Health and Human Services (HHS), rely on both their private networks and on the public telecommunications network to conduct mission-critical business. For example, the route of an electronic Medicare payment may traverse several networks—those operated by the HHS, 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.

Recent nationwide telecommunications failures remind us of our dependence on telecommunications—and the fragility of complex communications systems. On April 13, 1998, a software error in a single switch caused a major carrier to fail nationwide. According to press reports, during the 24-hour outage, the carrier’s corporate customers were unable to complete critical network-based business; retailers were unable to authorize credit card payments; and financial institutions could not complete electronic transactions.

Another failure occurred on May 19, 1998, when a communications satellite went into an uncontrolled spin after failure of a control system. The satellite’s failure disrupted the operations of credit card authorization services, paging services for 80 to 90 percent of all pagers in the United States, and the distribution of television programs. While these failures were not caused by a Year 2000 problem, they illustrate the degree to which we depend upon reliable, available, interoperable telecommunications.

⁹A PBX is a telephone switch located on a customer’s premises that primarily establishes voice-grade circuits between individual users and the public switched telephone network. A PBX also provides switching within the customer premises local area.

Major disruption in the service provided by the public telecommunications network can affect millions of users and cause massive financial losses. The cost of disruptions and outages caused by noncompliant computer or telecommunications systems was discussed in a recent study of the potential impact of Year 2000-related foreign exchange settlement failures.¹⁰ According to the study, the market costs of a single major bank's inability to settle its trades could reach \$3.3 billion in a single week. Business dependence on the public telecommunications infrastructure is particularly evident in the retail and financial sectors, where financial transactions with a combined value in the billions of dollars are made every day. Businesses and financial institutions rely heavily on telecommunications networks to participate in the global payments system, to exchange information with trading partners and regulatory agencies, and to manage their internal control systems and sophisticated computer equipment.

The consequences of not resolving Year 2000 problems in the telecommunications infrastructure are broad-based and potentially disastrous. For example, if critical telecommunications systems fail:

- The Internal Revenue Service would be unable to receive electronic tax returns or process electronic tax refunds.
- HHS would be unable to make electronic Medicare payments.
- Financial institutions and brokerages would be unable to process financial transactions and trades.
- The manufacturing and retail sectors would be unable to manage inventories.
- Air travel would have to be severely curtailed because air traffic control systems would fail.
- Credit card transactions would be hindered if communications links with point-of-sale systems fail.
- Emergency services would suffer if 911 calls were not properly and promptly routed.
- International voice and data services would be disrupted.

Telecommunications problems can affect virtually all network components—switches, routers, PBXs, and Internet servers—all of which must be assessed and tested. Compounding the risk is the global nature of today's telecommunications, which rely on seamless connections among widely scattered and widely diverse networks.

¹⁰Sustaining Stable Financial Markets Through the Millennium, Computer Sciences Corporation.

Federal Activity Related to the Year 2000 Readiness of the Telecommunications Sector

In light of the potential risks involved, the federal government has recently begun to address the Year 2000 readiness of the telecommunications sector. The government is undertaking telecommunications initiatives from three perspectives: national, international, and governmental.

National Initiatives

On February 4 of this year, the President's Council on Year 2000 Conversion was created, with the mandate to cooperate with private-sector operators of critical national and local systems, including telecommunications, in addressing the Year 2000 crisis. The council's recently established telecommunications working group—chaired by a Federal Communications Commission (FCC) commissioner—held its first meeting on April 29, 1998; membership includes representatives of the Departments of Agriculture, Commerce, Defense, and State; FCC; the General Services Administration (GSA); and the National Science Foundation. The group reports that it is developing a strategy and an action plan to address the key issues facing the telecommunications sector. These include raising industry awareness of the problem and disseminating information on best practices and contingency planning.

In addition to its role on the council, within the past 2 months FCC has established a Year 2000 Internet web site, formed a task force to coordinate the activities of FCC bureaus to provide Year 2000 information for consumers and industry, and coordinated an outreach effort to state public utility commissions. Its specific national efforts are focusing on raising the Year 2000 awareness of companies under its jurisdiction, monitoring the status of Year 2000 readiness of the telecommunications sector, and helping telecommunications users obtain information from individual telecommunications service providers needed for testing.

As part of this campaign, FCC in late April sent letters to over 200 telecommunications service providers, industry associations, and other interested organizations, advising them of the seriousness and potential impact of the Year 2000 problem and asking them to share information about the Year 2000-compliance status of their services with FCC, others in the telecommunications industry, and the public—including making such information available on the Internet. FCC is also contacting additional service providers and equipment manufacturers, and is working with industry associations to reach the hundreds of small and midsized telecommunications service providers.

The Securities and Exchange Commission also has an initiative to gather information on companies' Year 2000 activities. In October 1997 and January 1998, the Commission urged public operating companies (which would include those in the telecommunications sector) to disclose their anticipated costs, problems, and uncertainties associated with the Year 2000 issue.

International Initiatives

FCC is also working on the international front, by coordinating with the International Telecommunications Union to reduce the risk of disruption to international telecommunications services. In addition, the Department of State has initiated discussions between embassies and public telecommunications network providers worldwide to determine the potential impact of the Year 2000 problem. In July 1997, the department's Diplomatic Telecommunications Services Program Office sent a cable to foreign posts asking them to determine whether the local telecommunications carriers—the national post, telephone, and telegraph companies—are aware of the problem and whether they are making plans to ensure the availability of telecommunications services on January 1, 2000.

Governmental Initiatives

Year 2000 actions concerning the federal government's telecommunications networks have been initiated by the Chief Information Officers (CIO) Council's¹¹ Year 2000 Committee, GSA, and federal agencies. The CIO Council Year 2000 Committee has a telecommunications subcommittee to focus on telecommunications issues in addressing the Year 2000 problem. This subcommittee, chaired by GSA, has adopted a Year 2000 telecommunications compliance program that lays out a framework, including milestones, for agencies to use in addressing telecommunications issues. This compliance program also focuses on enhancing partnerships with industry to identify Year 2000-compliant products and services, develop test methodologies and processes, perform collaborative testing of network elements/systems, and share compliance information and test results. The subcommittee is also addressing contingency planning for telecommunications.

In addition to its role chairing the Subcommittee on Telecommunications, GSA owns, manages, or resells consolidated telecommunications services

¹¹The CIO Council comprises CIOs and Deputy CIOs from 28 large federal departments and agencies, two CIOs from small federal agencies, agency representatives from the Office of Management and Budget, and the Chairs of the Government Information Technology Services Board and Information Technology Resources Board.

to federal agencies throughout the United States; it controls about 25 percent of all federal telecommunications services. GSA's Year 2000 program addresses three service areas: Federal Telecommunications System (FTS 2000)¹² services, other federal telecommunications services, and commercial services. In the FTS 2000 area, GSA plans to complete assessment of Year 2000 compliance by this September, renovation by March 1999, and validation and testing between April and December 1999. In the other federal services area, GSA is supporting agencies in hardware testing, is conducting Year 2000 telecommunications working group meetings with agency representatives, and is managing its Year 2000 web site. In the area of commercial services, GSA plans by March 1999 to conduct interoperability testing between government systems and network service providers.

Issues Surrounding Year 2000 Telecommunications Readiness

Key federal initiatives are in their early stages on a national, international, and governmental level, and critical issues remain to be addressed. Less than 19 months remain, yet no one currently has an overall assessment of the degree of Year 2000 risk in the telecommunications infrastructure. Accordingly, it is imperative that the executive branch, and particularly FCC and the Conversion Council's telecommunications working group, take a more active approach to addressing the Year 2000 issues of the domestic and international telecommunications sectors.

National Issues

The federal government is uniquely positioned to publicize the Year 2000 computing crisis as a national priority; take a leadership role; and identify, assess, and report on the risks and necessary remediation activities associated with the nation's key economic sectors, such as telecommunications. Accordingly, in an April 1998 report, we recommended that the President's Council on Year 2000 Conversion

establish public/private partnership forums composed of representatives of each major sector that, in turn, would rely on task forces organized along economic sector lines to 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 assure the continuing delivery of critical public and private services.¹³

¹²FTS 2000 is a nationwide telecommunications network providing long-distance voice and data services to federal agencies.

¹³Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

In disagreeing with this recommendation, the Chair of the Conversion Council stated his belief that the council needs to be a catalyst, facilitator, and coordinator. He did, however, establish five new working groups—telecommunications among them; while not providing specific guidelines or expectations, the Chair told them to focus on developing a coordinated outreach plan and establish communications with public and private parties within each sector, and to monitor the Year 2000 readiness of each sector.

Given the inarguably critical nature of telecommunications services to the functioning of our nation, coordinated oversight is essential. In order to gain confidence that our telecommunications infrastructure will be ready for the next century, accountability must be established; this includes a broad strategy as well as specific milestones and defined accountability.

We see several major areas that must be addressed: (1) obtaining information on the current readiness status of various segments of the telecommunications industry for the next century, (2) establishing a mechanism for obtaining such readiness information on a regular basis, (3) setting milestones for achieving Year 2000 compliance, (4) disseminating readiness status information to the public and the Congress, and (5) developing—in conjunction with the private sector—contingency plans to ensure business continuity, albeit at reduced levels, in the event that not all telecommunications systems are fully operational on January 1, 2000.

Current Status

Based on data from industry associations and telecommunications companies, FCC has compiled general information on the status and activities of various segments of this sector. In late April of this year, the agency asked the telecommunications industry for Year 2000-compliance information; however, as of last week, FCC was unable to provide us with information on the current status and anticipated readiness dates in areas such as satellite, cable, broadcast, and wireless services. As a major example, FCC could not provide us with data on when major interexchange (long distance) and local exchange carriers were expecting to be Year 2000 compliant.

Because FCC did not have such data readily available, we attempted to obtain Year 2000 milestone information from the major interexchange (long distance) and local exchange carriers. We focused on these 12 carriers because they hold key positions within the telecommunications

sector and account for over 90 percent of the market.¹⁴ We obtained this information from the carriers' World Wide Web sites, or through telephone interviews with carrier representatives.

Table 1 provides a summary of the information we gathered. The table shows that most major carriers expect to achieve Year 2000 compliance of their networks by December 1998, although for some it is either later than that date or we were unable to obtain this information. The table also shows that most major carriers plan to be fully compliant—including support systems—by mid-1999.

Table 1: Year 2000-Compliance Status of Major Telecommunications Carriers

Service providers	Date expected to be Year 2000 compliant	
	Network services ^a	Support services ^b
Interexchange carriers		
AT&T	December 1998	June 1999
Excel	(did not respond)	(did not respond)
Frontier	December 1998	December 1998
MCI	December 1998	June 1999
Sprint	December 1998	June 1999
Worldcom	April 1999	April 1999
Local exchange carriers		
Ameritech	January 1999	January 1999
Bell Atlantic	July 1999	(not specified)
BellSouth	December 1998	December 1998
GTE	December 1998	December 1998
SBC	December 1998	December 1998
Sprint	December 1998	June 1999
US West	June 1999	June 1999

^aNetwork services are key systems and network elements affecting customer services.

^bSupport services are services and systems supporting carrier operations.

Source: Individual carriers. We did not independently verify this information.

In addition to the individual carrier information shown in the table, some interoperability testing is planned. This laboratory-based testing, sponsored by the Telco Year 2000 Forum and by the Alliance for Telecommunications Industry Solutions (ATIS), is scheduled to begin later this year and continue throughout 1999. The forum-sponsored testing will

¹⁴According to FCC, there are over 1,300 companies that provide local telephone service in the United States. More than 700 firms buy access from these companies.

focus on interoperability between local exchange carriers, while the ATIS-sponsored tests will focus on common equipment interoperability between a local exchange carrier and a long-distance carrier.

Recurring Status Information

Not only is it important that FCC know the current status of telecommunications preparedness, it is imperative that such information be obtained on a regular basis. Just as the Office of Management and Budget (OMB) and the Congress monitor individual agency progress through quarterly reports on the status of Year 2000 systems compliance, FCC would benefit from a mechanism that would provide updated status data on a recurring basis. Without this information, FCC will find it more difficult to address major problems that may occur. FCC's recent letters to the industry are a start, but ongoing receipt of information will be essential to effectively monitor sector readiness.

Milestone Setting

While telecommunications service providers are establishing their own Year 2000 schedules, FCC has not developed schedules and milestones for the various segments of the telecommunications industry to achieve Year 2000 compliance. Milestones for activities such as renovation, validation, and implementation are important to overall Year 2000 telecommunications planning and for evaluating progress in reaching compliance.

Information Dissemination

Beyond obtaining current and ongoing status information, it is important that FCC make such information available to the public—including telecommunications customers—and the Congress. The dissemination of this information could provide continuous information about the preparedness of this essential sector for the century change. Potential vehicles for such dissemination include regular reports to the Congress.

Contingency Planning

Contingency plans should be formulated to respond to two types of failures: predictable (such as repairs or replacements that are already far behind schedule) and unforeseen (such as a system that fails despite having been certified as Year 2000 compliant or one that, it is later found, cannot be corrected by January 1, 2000, despite appearing to be on schedule today). Given the central nature of telecommunications to the ability of other sectors to be Year 2000 ready, a public/private partnership could be formed to develop and test necessary contingency plans, critical to ensuring the continuity of service in the event of failures.

International Issues

Little is known about the Year 2000 readiness of foreign telecommunications carriers and their ability to continue to provide telecommunications services after December 31, 1999. In September 1997, the Gartner Group conducted several surveys to determine how companies around the world were dealing with the Year 2000 problem. The study did not focus on the telecommunications sector; however, its findings provide an indication of the overall Year 2000 readiness of the various geographic regions of the world. According to the study, “[t]hirty percent of all companies have not started dealing with the year 2000 problem. Small companies, health care organizations, educational institutions, and many companies in 30 percent of the world’s countries are at a high risk of seeing year 2000 mission-critical failures due to a lack of readiness.”¹⁵ A more recent survey focusing on foreign telecommunications service providers was conducted by the International Telecommunication Union; its results are not yet available.

FCC has also noted that Year 2000 issues have not received the same level of attention abroad as in the United States, with the exception of the United Kingdom. This was confirmed by the results of the State Department’s initiative to assess the Year 2000 readiness of foreign carriers. As shown in table 2, the department received information from 113 countries, updated through March 1998. Of those, 25 countries (22 percent) expected to be compliant by this December; 26 countries (23 percent) expected to be compliant by December 1999; 33 countries (29 percent) stated that they were addressing the Year 2000 issue but were having problems; and 29 countries (26 percent) were unaware of or had not begun to address the problem. The State Department is continuing its activities to determine the Year 2000 readiness of its foreign posts, and is developing contingency plans to ensure continuity of diplomatic telecommunications services.

¹⁵Year 2000-World Status (Gartner Group, Document #M-100-037, November 25, 1997).

Table 2: Year 2000-Compliance Status of International Post, Telephone, and Telegraph Companies

Region	Compliance expected by the end of 1998	Compliance expected by the end of 1999	Addressing Year 2000, but having problems	Unaware or not begun	Total
Central and South America	4	2	4	5	15
Europe and Canada	8	15	9	9	41
Africa	2	1	10	9	22
East Asia and the Pacific	8	6	5	4	23
Near East and South Asia	3	2	5	2	12
Total	25	26	33	29	113
Percentage	22%	23%	29%	26%	100%

Source: Department of State. We did not independently verify this information.

The World Bank is reporting similar findings. In an informal survey of foreign Year 2000 readiness conducted this month, only 18 of 127 countries (14 percent) had a national Year 2000 program; 28 countries (22 percent) report working on the problem; and 16 countries (13 percent) report only awareness of the issue. No conclusive data were received from the remaining 65 countries surveyed (51 percent). The World Bank is now planning to appoint a field Year 2000 representative for each country.

The Year 2000 readiness of international telecommunications networks and carriers is clearly an area of concern. All sectors of the global economy depend upon reliable communications networks to handle billions of dollars in financial transactions. Current and ongoing information to monitor the compliance status of foreign carriers would, therefore, allow the federal government and the private sector to identify troubled regions and develop contingency plans for ensuring the continuity of vital telecommunications services.

Governmental Issues

Without compliant telecommunications, federal agencies will be unable to provide basic services to the American public. However, many major departments and agencies do not yet know the Year 2000 compliance status of their own telecommunications networks and services. In fact, many federal agencies are just beginning to assess the readiness of their telecommunications. As of last month's quarterly reports to OMB, only 11 of 24 major federal agencies reported that they had completed inventories and/or assessments of telecommunications. The Department of

Agriculture, for example, does not expect to complete its telecommunications inventory until next month—a critical assessment task that should have been completed last summer.

In closing, let me reiterate that the importance of the telecommunications infrastructure in the successful functioning of our nation cannot be overemphasized; it is the linchpin of our economy and critical citizen services. Yet the telecommunications industry faces a massive challenge to make sure that it can finish the Year 2000 job in time. While the federal government must take a stronger, more active oversight role to help ensure that this central sector is prepared, much of the responsibility inevitably lies with the industry and other countries around the world.

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

GAO Reports and Testimony Addressing the Year 2000 Crisis

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).

National Weather Service: Budget Events and Continuing Risks of Systems Modernization ([GAO/T-AIMD-98-97](#), March 4, 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).

USDA Information Management: Extensive Improvements Needed in Managing Information Technology Investments ([GAO/T-AIMD-97-90](#), May 14, 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

