United States General Accounting Office

GAO

Testimony

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

YEAR 2000 COMPUTING CRISIS

Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs

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

Madam Chairwoman and Members of the Subcommittee:

We are pleased to be here today to discuss the computing challenges that the upcoming change of century poses to virtually all major organizations, public and private, including government programs with a high degree of interaction with the American public such as the Social Security Administration (SSA) and Medicare. As the world's most advanced and most dependent user of information technology, the United States possesses close to half of all computer capacity and 60 percent of Internet assets.[1] As a result, the coming century change presents a particularly sweeping and urgent challenge for entities in this country.[2]

For this reason, we have designated the Year 2000 computing problem as a high-risk area[3] for the federal government, and have published guidance[4] to help organizations successfully address the issue. Since early 1997 we have issued over 35 products detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[5]

The common theme of these reports has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness. 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 creation of the President's Council on Year 2000 Conversion represents an opportunity to orchestrate the leadership and public/private

---

[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]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997) and Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, March 1998 [exposure draft]).

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

partnerships essential to confronting the unprecedented challenges that our nation faces. My testimony today will briefly outline our views on what additional actions must be taken to reduce the nation's Year 2000 risks, and what our inquiries into Year 2000 readiness found at Social Security, the Health Care Financing Administration (HCFA) and Medicare, and at the Department of the Treasury.

Risk of Year 2000 Disruptions Requires Leadership

The public faces the 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 the levels of governments and within key economic sectors of our nation could cause a single failure to have wide-ranging repercussions. While managers in the government and the private sector are acting to mitigate these risks, a significant amount of work remains.

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 many of the government's existing systems and its lackluster track record in modernizing systems to deliver expected improvements and meet promised deadlines.

Year 2000-related problems have already occurred. 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.[6]

Our reviews of federal agency Year 2000 programs have found uneven progress, and our reports contain numerous recommendations, which the agencies have almost universally agreed to implement. Among them are the need to establish priorities, solidify data exchange agreements, and develop contingency plans.

One of the largest, and largely unknown, risks relates to the global nature of the problem. With the advent of electronic communication and

---

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

international commerce, the United States and the rest of the world have become critically dependent on computers. However, with this electronic dependence and massive exchanging of data comes increasing risk that uncorrected Year 2000 problems in other countries will adversely affect the United States. And there are indications of Year 2000 readiness problems internationally. In September 1997, the Gartner Group, a private research firm acknowledged for its expertise in Year 2000 computing issues, surveyed 2,400 companies in 17 countries and concluded that "[t]hirty percent of all companies have not started dealing with the year 2000 problem."[7]

Additional Actions Must Be Taken to Reduce Nation's Year 2000 Risks

As 2000 approaches, the scope of the risks that the century change could bring has become more clear, and the federal government's actions have intensified. This past February, an executive order was issued establishing the President's Council on Year 2000 Conversion. The Council Chair is to oversee federal agency Year 2000 efforts as well as be the 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.

As we testified in March,[8] there are a number of actions we believe the Council must take to avert this crisis. In a report issued just last week, we detailed specific recommendations.[9] The following summarizes a few of the key areas in which we recommend action:

- Because departments and agencies have taken longer than recommended to assess the readiness of their systems, it is unlikely that they will be able to renovate and fully test all mission-critical systems by January 1, 2000. Consequently, setting priorities is essential, with the focus being on systems most critical to our health and safety, financial well being, national security, or the economy.
- Agencies must start business continuity and contingency planning now to safeguard their ability to deliver a minimum acceptable level of services in the event of Year 2000-induced failures. In March we issued an exposure draft of a guide providing information on business continuity and contingency planning issues common to most large enterprises; OMB

---

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

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

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

recently adopted this guide as a model for federal agencies.[10] Agencies developing such plans only for systems currently behind schedule, however, are not addressing the need to ensure business continuity in the event of unforeseen failures. Further, such plans should not be limited to the risks posed by the Year 2000-induced failures of internal information systems, but must include the potential Year 2000 failures of others, including business partners and infrastructure service providers.

- The Office of Management and Budget's (OMB) assessment of the current status of federal Year 2000 progress is predominantly based on agency reports that have not been consistently verified or independently reviewed. Without such independent reviews, OMB and the President's Council on Year 2000 Conversion have little assurance that they are receiving accurate information. Accordingly, agencies must have independent verification strategies involving inspectors general or other independent organizations.

- As a nation, we do not know where we stand overall with regard to Year 2000 risks and readiness. No nationwide assessment—including the private and public sectors—has been undertaken to gauge this. In partnership with the private sector and state and local governments, the President's Council could orchestrate such an assessment.

Social Security Administration

At this point I would like to address our findings at specific agencies, beginning with the Social Security Administration. We see significant progress at SSA, and it is essential that this progress continue. SSA has been anticipating the change of century since 1989, initiating an early response to the potential crisis. It made important early progress in assessing and renovating mission-critical mainframe systems—those necessary to prevent the disruption of benefits—and has been a leader among federal agencies.

Three key risks remained, however, as discussed in our report of last October and testimony of this past March.[11] One major risk concerned Year 2000 compliance of the 54 state Disability Determination Services (DDS)[12] that provide vital support to the agency in administering SSA's disability programs. The second major risk concerned data exchanges,

---

[10]GAO/AIMD-10.1.19, March 1998 [exposure draft].

[11]Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997) and Social Security Administration: Information Technology Challenges Facing the Commissioner (GAO/T-AIMD-98-109, March 12, 1998).

[12]One for each state plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. A federal DDS serves as a backup and model office for testing new technologies and work processes.

ensuring that information obtained from these thousands of outside sources—such as other federal agencies, state agencies, and private businesses—was not "corrupted" by data being passed from systems not Year 2000 compliant. Third, such risks were compounded by the lack of contingency plans to ensure business continuity in the event of systems failure.

We recommended several specific actions to mitigate these risks. These included (1) strengthening monitoring and oversight of state DDS Year 2000 activities, (2) expeditiously completing the assessment of mission-critical systems at DDS offices and using those results to establish specific plans of action, (3) discussing the status of DDS Year 2000 activities in SSA's quarterly reports to OMB, (4) quickly completing SSA's Year 2000 compliance coordination with all data exchange partners, and (5) developing specific contingency plans that articulate clear strategies for ensuring the continuity of core business functions.

At the request of this Committee's Subcommittee on Social Security and the Senate Special Committee on Aging, we are monitoring SSA's implementation of our recommendations. SSA has agreed with all of our recommendations, and actions to implement them have either been taken or are underway.

Regarding state DDSs, SSA has enhanced its monitoring and oversight by establishing a full-time DDS project team, designating project managers and coordinators, and requesting biweekly status reports. Further, almost all states have now submitted initial Year 2000 plans; SSA now reports that 22 DDSs have had their systems renovated\ tested, and implemented. In addition, beginning with its November 1997 report, SSA has included information on DDSs in its quarterly reports to OMB.

SSA has also identified its external data exchanges and is in the process of coordinating with its partners to make the exchanges Year 2000 compliant. Further, SSA began working with the Department of the Treasury in March of this year to test for the disbursement of benefit checks and other direct deposit payments.

Finally, in accordance with our guidance, SSA has completed a high-level, overall plan for business continuity. This plan represents a sound framework from which SSA can build its specific contingency plans. These specific plans—for each core business area—need to be developed to ensure that operations continue uninterrupted.

Medicare and the Health Care Financing Administration

As the nation's largest health insurer, Medicare expects to process over a billion claims and pay $288 billion in benefits annually by 2000. The consequences, then, of its systems' not being Year 2000 compliant could be enormous. In a report issued last May,[13] we discussed the critical managerial and technical challenges facing the Health Care Financing Administration (HCFA) in its efforts to ensure the viability of systems to handle Medicare transactions into the next century.

We found that HCFA had not required systems contractors to submit Year 2000 plans for approval. Further, it did not have contracts or other specific legal agreements with any contractors, other than one recently selected contractor, stating how or when the Year 2000 problem would be corrected, or whether contractors would certify that they would correct the problem.

HCFA had also not identified critical areas of responsibility for Year 2000 activities. Although HCFA's regional offices have a role in overseeing contractor efforts, their specific Year 2000 responsibilities had not been defined, nor had guidance been prepared on how to monitor or evaluate contractor performance. While HCFA had been assessing the impact of the century change on its internal systems, it had not completed a similar review of Medicare contractors' claims processing systems. Further, HCFA had not required its contractors to prepare an assessment of the severity of impact of potential Year 2000 problems.

Plans for independent validation of contractors' strategies and test plans were also lacking. Likewise, while HCFA had asked contractors to identify their system interfaces, it had no plans for approving the contractors' approaches for addressing interface and data exchange issues. Moreover, HCFA had not developed contingency plans to address continuity of business operations in the event of Year 2000-induced failures. HCFA officials were again relying on the contractors themselves to identify and complete the necessary work in time to avoid problems. Yet the contractors had not developed contingency plans—and did not intend to—because they considered this HCFA's responsibility.

To address these deficiencies in HCFA's approach, we made several recommendations to the Secretary of Health and Human Services. These included identifying responsibilities for managing and monitoring Year 2000 actions, preparing an assessment of the severity of impact and timing

---

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

of potential Year 2000 problems, and developing contingency plans. We also recommended that HCFA require its contractors to submit for review and approval (1) plans for identifying and correcting potential problems, including certification that their changes would correct the problems, (2) validation strategies and test plans for systems, and (3) plans for addressing interface and data exchange issues.

The Department of Health and Human Services (HHS) has agreed to implement our recommendations. For example, HCFA has established the position of Chief Information Officer (CIO); this individual has made the Year 2000 issue his top priority. HCFA has also established a Year 2000 organization, and the issue is included in HCFA's information technology investment process and annual performance plan goals. It is also developing business continuity and contingency plans, with a draft plan set for release this month. Further, the Medicare carriers' manual has been revised to require such contingency planning.

It should be noted, however, that since our report of last year,[14] HHS' and OMB's concerns about the Medicare contractors' systems have become more evident. For example, according to HHS' February 1998 quarterly Year 2000 report, "HCFA's Medicare contractor systems continue to be of great concern to the Department." In addition, in its summary of all agencies' February 1998 reports, OMB concluded that HHS was making insufficient progress on Year 2000 due in large part to HCFA's delays.

There are also indications that the agency has not documented the severity of impact of Year 2000-related failures—in other words, how its core business functions would be affected if its automated information systems failed because of Year 2000-related problems. For example, if Medicare systems failed, the number of health services providers who would not be paid, paid late, or in incorrect amounts is unknown. HCFA has recently begun contingency planning that may address some of these issues. We are currently evaluating the effectiveness of HCFA's actions, at the request of the Senate Special Committee on Aging.

Department of the Treasury

With respect to the Department of the Treasury, we must first point out that—unlike with Social Security and Medicare—we have not completed a thorough assessment of the Department's Year 2000 readiness. However, we can describe some of what we have seen, and what Treasury officials themselves report. In addition, we have undertaken detailed work at the

---

[14]GAO/AIMD-97-78, May 16, 1997.

Internal Revenue Service (IRS), which will be discussed in a separate statement today.

Treasury's role in delivering government services, such as Social Security and Medicare payments, is vital. Treasury's Financial Management Service (FMS), for instance, as the government's cash receipts and disbursements agent and financial manager, represents the crossroads of financial activity for the federal government. However, the Department's progress in making systems Year 2000 compliant has been mixed. Bureaus such as its Office of Thrift Supervision are making good progress in converting their systems and in overseeing the conversion activities of the financial institutions that they regulate and inspect.[15] In contrast, FMS is falling seriously behind schedule in converting some of its systems.[16] Treasury Year 2000 program officials are aware of these and other related risks facing the Department, and have established program management structures and processes to address them, which we are presently evaluating.

To perform their core business functions, Treasury and its bureaus rely on a vast—and in many cases antiquated—collection of systems, thereby complicating Year 2000 renovations. To integrate many of the bureaus' systems and permit them to interact and exchange information with a wide assortment of federal, state, and local government and private-sector data exchange partners (over 6,800, according to the Department), Treasury operates and maintains the largest non-Defense telecommunications network in the federal government.

The responsibilities of Treasury's Year 2000 program office are basically twofold: guiding, monitoring, and reporting on the conversion activities of its bureaus; and converting and reporting on Departmentwide telecommunications systems that support its bureaus. To guide, monitor, and report on bureau activities, Treasury has (1) established a departmental program office and designated a program manager within the CIO organization, (2) established Year 2000 working groups and designated work group project managers to focus on major categories of

---

[15]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).

[16]Treasury encompasses 14 separate bureaus or program offices. Two of these—the Internal Revenue Service (IRS) and the U.S. Customs Service—account for almost 98 percent of federal revenues each year. Two other major bureaus for which Year 2000 compliance implications are critical include FMS and the Bureau of the Public Debt. Taken together, these four bureaus are instrumental in the efficient collection and payment functions that support beneficiaries of programs such as Social Security and Medicare.

systems, (3) issued a departmental Year 2000 conversion strategy, guidance, and standards, and (4) established monthly progress reporting requirements. Additionally, it used its existing CIO Council as a forum for Year 2000 information exchanges between the Department and bureau CIOs, hired a contractor to validate the information being reported by its bureaus, and developed draft guidance governing the process to be used in certifying systems as compliant and for verification and validation of certification determinations.

As a result of this program office oversight, Treasury has a good appreciation of where its attention must be focused. Program officials recognize that progress among the bureaus has been uneven, as has progress within individual agencies for certain categories of systems. For example, they stated that FMS is Treasury's highest priority because of its slow progress to date and the criticality of its role in managing the government's finances. As a result, according to the Department's Year 2000 program manager, FMS progress and activities are tracked on a daily basis and, consequently, FMS Year 2000 management effectiveness has improved.

Department Year 2000 officials further report that telecommunications systems and non-information technology (IT) areas, such as systems embedded in facilities and equipment, are not as far along as other IT areas, such as financial and management information systems, because work in these areas started late. To address this risk, Treasury has established working groups and project managers for both telecommunications and non-IT systems, along with formal processes for guiding, monitoring, and reporting on these areas.

To address the conversion of its telecommunications systems, the program office has established a telecommunications working group and designated a project manager. A risk management plan has also been established, as has a test facility to permit all telecommunications systems components to be tested before being placed in operation. In addition, a contractor has been hired to perform independent verification and validation of telecommunications conversion activities.

Despite these actions, Treasury and its bureaus face other major risks that must be managed effectively if key systems are to be ready in time. For example, the assessment phase—during which the compliance of mission-critical systems is determined—has not been completed. This is worrisome because it reduces the amount of time left for critical

renovation, validation, and implementation activities. Treasury's milestone for assessing all mission-critical systems was July 1997. However, as of the end of March 1998, FMS still had not completed assessing the compliance of five of its mission-critical systems. For example, according to Treasury's latest status report, FMS is awaiting a contractor proposal for renovating a system called GOALS I—for Government On-Line Accounting Link System I. This system plays a critical role in processing interagency payments and collections. Of particular note is that the need to assess GOALS I for renovation arose only recently, when it became apparent that GOALS II, intended to replace GOALS I, will not be ready in time.

For non-IT systems, Treasury's components are farther behind. As of mid-March, systems in 3 of Treasury's 14 bureaus had still not been inventoried. Of the systems in the 11 inventoried bureaus, many remain to be assessed.

A final risk area is that contingency plans for ensuring continuity of business operations have not yet been developed. As our guidance points out,[17] business area priorities and system dependencies must be examined in light of possible Year 2000-induced failures; contingency planning to help ensure continuity of business operations must then be developed and tested.

Although Treasury's Year 2000 program office recognizes the importance of business continuity planning and has issued guidance in this area, bureaus have not yet completed such plans, and are at risk of being unable to complete them in time. For example, IRS plans to develop contingency plans only for those business areas relying on systems whose conversions are behind schedule. With this approach, IRS will have no ready response to unexpected Year 2000-induced problems. Further exacerbating this problem is that devising and activating manual or contract processes to ensure continuity of operations could be a daunting task. According to a Treasury contractor, it may be difficult for some Treasury components, such as FMS, to formulate an approach to operating in a nonautomated environment.

In conclusion, the change of century will present many difficult challenges in information technology and in ensuring the continuity of business operations, and has the potential to cause serious disruption to the nation and to government entities on which the public depends, including SSA,

---

[17]GAO/AIMD-10.1.19, March 1998 [exposure draft].

Medicare, and Treasury. These risks can be mitigated and disruptions minimized with proper attention and management. While these agencies and programs have been working to mitigate their Year 2000 risks, further action must be taken to ensure continuity of mission-critical business operations. Continued congressional oversight through hearings such as this can help ensure that such attention is sustained and that appropriate actions are taken to address this crisis.

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

GAO Reports and Testimony Addressing the Year 2000 Crisis

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: 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 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).