United States General Accounting Office

GAO

Testimony

Before the Committee on Resources,
House of Representatives

For Release on Delivery
Expected at
11 a.m.
Wednesday,
April 22, 1998

DEPARTMENT OF THE INTERIOR

Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations

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

GAO/T-AIMD-98-149

Mr. Chairman and Members of the Committee:

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 the Department of the Interior. 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 the United States.[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 30 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 recent creation of the President's Council on Year 2000 Conversion represents an opportunity to orchestrate the leadership and public/private partnerships essential to confronting the unprecedented

[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, Exposure Draft, March 1998).

[5]A listing of our publications is included at the end of this statement.

challenges we face. My testimony today will briefly outline where the federal government stands in its efforts to lessen Year 2000 risks. I will then present our preliminary observations on Year 2000 activities at the Department of the Interior.

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 international commerce, the United States and the rest of the world have become critically dependent on computers. However, with this electronic

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

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 Can 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 last month,[8] there are a number of actions we believe the Council must take to avert this crisis. We plan to issue a report later this month detailing our specific recommendations. The following summarizes a few of the key areas in which we will be recommending 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. Last month, we issued an exposure draft of a guide providing information on business continuity and contingency planning issues common to most large enterprises.[9] 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

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

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 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.

Observations on Interior's Year 2000 Approach

Ensuring that information systems are made Year 2000 compliant is an enormous, difficult, and time-consuming challenge for a large organization such as the Department of the Interior. Interior's systems support a wide range of programs; unless they can function into the next century, the department is at risk of being unable to effectively or efficiently carry out its critical missions.

As the nation's principal conservation agency, Interior has responsibility for managing most of our nationally owned public lands and natural resources, protecting our fish and wildlife, and preserving the environmental and cultural values of our national parks and historic places. The department's core business processes could fail—in whole or in part—if supporting information systems are not made Year 2000 compliant in time. These include systems that

- account for and disburse mineral royalties of about $300 million each month,
- support the management of the nation's lands and mineral resources,
- account for and maintain records on over $2.5 billion of American Indian trust fund assets, and
- detect and analyze ground motion and provide early warnings of earthquakes.

A detailed example of this kind of risk can be seen in recent work we performed for the House Committee on Appropriations, Subcommittee on Interior and Related Agencies, where we concluded that recent and potential future delays in the Bureau of Land Management's (BLM) Automated Land and Mineral Record System (ALMRS) introduce the risk that BLM will lose information systems support for some core business processes. Two systems that ALMRS is scheduled to replace, the Case Recordation System and the Mining Claim Recordation System, are currently not Year 2000 compliant. BLM uses these two systems to create and manage land and mineral case files. They capture and provide information on case type, customer, authorizations, and legal descriptions. Without these systems, BLM cannot create and record new cases, such as mining claims, or update case information.

Delays in implementing ALMRS introduce the risk that BLM will be forced to continue using these two systems beyond 2000. To mitigate this risk, BLM has begun planning to ensure that these two systems can run in 2000 and beyond, if necessary. BLM has not yet, however, completed its assessment to determine what specific actions are needed to accomplish this, nor has it developed a contingency plan to ensure the continuity of core business processes in the event that ALMRS is not fully deployed by 2000. In a draft report to be released soon, we are recommending that BLM assess the systems to be replaced by ALMRS to determine what actions are needed to ensure their continued use after January 1, 2000, and develop a contingency plan should ALMRS not be fully and successfully deployed in time.

Interior officials have stated that they recognize the importance of ensuring that their systems are Year 2000 compliant. The Secretary has said that identifying and correcting Year 2000 computer problems is a priority, and the former Chief Information Officer called this challenge one of the most serious operational and administrative problems the department has ever faced. In assessing the magnitude of the problem, the department's bureaus and offices identified 95 mission-critical systems,[10] with a total of about 18 million lines of software code, all of which must be examined. Interior estimates that correcting these 95 systems will cost $17.3 million, as shown in the following table.

[10]Interior defines mission-critical systems to be those that, when their capabilities are degraded, the organization realizes a resulting loss of a core capability or life or property are threatened.

Table 1: Number of Interior Mission-Critical Systems as of February 1998

Component organization	Total number of mission-critical systems	Estimated cost to correct
Bureau of Indian Affairs	15	$5,545,000
U.S. Geological Survey	15	2,706,000
Office of the Secretary	11	2,503,000
National Park Service	2	2,310,000
Minerals Management Service	4	2,060,000
Office of Surface Mining	16	850,000
Bureau of Land Management	15	690,000
Bureau of Reclamation	16	439,000
U.S. Fish and Wildlife Service	1	246,000
Total	**95**	**$17,349,000**

Source: Department of the Interior. We did not independently verify these data.

In addition to these systems, the department is also assessing its communications systems and embedded computer chip technologies to determine whether they will be affected by the coming century change. Embedded systems are special-purpose computers built into other devices. Many facilities used by the federal government that were built or renovated within the last 20 years contain embedded computer systems to control, monitor, or assist in operations. If the embedded chips used in such devices contain two-digit date fields for year representation, the devices could malfunction. For example, control systems that regulate water flow and generators in our nation's dams, which produce over 42 billion kilowatts of energy each year, could fail.

Interior's Year 2000 program operates in a decentralized fashion as its bureaus and offices are responsible for identifying and assessing their mission-critical systems, determining correction priorities, and making their own mission-critical systems Year 2000 compliant. Departmental oversight is provided by Interior's Year 2000 Project Office. This office reports directly to the Chief Information Officer.

The Year 2000 Project Team consists of a Year 2000 coordinator from the department and a representative located in each bureau or office. The bureaus and offices maintain information used to manage their Year 2000 activities. Bureau and office representatives submit monthly milestone and status information to the coordinator, which he analyzes and compiles manually. The coordinator tracks major milestones, such as systems assessments completed, Year 2000 renovations completed, and systems

implemented. The information is forwarded to the Chief Information Officer and, each quarter, to OMB.

According to Interior's Year 2000 coordinator, he tracks the 95 mission-critical systems and maintains status information in a word processing table that lacks the capability for automated tracking or analysis. He stated that he notifies the Chief Information Officer of any reported milestone delays, which are then discussed at senior-level management meetings. Table 2 shows the status of the 67 mission-critical systems that are being renovated, as reported to OMB on February 15, 1998. (This table does not include the other 28 mission-critical systems, which are considered already compliant or are being replaced.)

Table 2: Status of 67 Mission-Critical Systems Being Renovated, as of February 15, 1998

	Assessment	Renovation	Validation	Implementation
Number Completed	67	32	22	19
Percentage Completed	100%	48%	33%	28%

Source: Department of the Interior. We did not independently verify these data.

Accurate reporting is critical to ensuring that executive management receives a reliable picture of the Year 2000 progress of component organizations. This is particularly important at Interior, where much of the Year 2000 program responsibility is delegated to the individual bureaus and offices. Although the department relies on its bureaus to provide monthly reports on the status of their Year 2000 renovation actions, to date it has not verified the accuracy and reliability of the reported information.

As the only staff member in Interior's Year 2000 Project Office, the department's coordinator does not have the ability to verify the accuracy of reported information on the bureaus' and offices' mission-critical systems. Therefore, the Chief Information Officer requested that Interior's Inspector General assist in monitoring the progress of the individual bureaus in achieving Year 2000 compliance.[11] It is important to verify because if the data are inaccurate, it will be more difficult to identify and correct problems promptly.

[11]The Inspector General began reviews of the Bureau of Indian Affairs, National Park Service, and Bureau of Reclamation in 1998; these are the department's first attempts to verify the status of the bureaus' and offices' Year 2000 efforts and management information.

Interior regularly exchanges data with other organizations. In many instances, these data are critical to the department's operations. In response to a recent survey we conducted, Interior reported that 40 of its 95 mission-critical systems exchange electronic data with other federal, state, and local agencies; domestic and foreign private sectors; and foreign governments. Although the bureaus have identified over 2,900 incoming and outgoing external data exchanges, the department does not have a central inventory. While it has asked each bureau and office head to certify that date-sensitive data exchanges have been identified and data exchange partners contacted to begin resolving date-format issues, the lack of a centralized inventory and an automated way to maintain it means that Interior could be missing key information showing whether exchange agreements are proceeding as scheduled. Failure to reach such agreements raises the risk that Interior's systems will receive noncompliant data that can corrupt its databases.

The risk of failure is not limited to an organization's internal information systems, but includes the potential Year 2000 failures of others, such as business partners. One weak link in the chain of critical dependencies and even the most successful Year 2000 program will fail to protect against major disruption of business operations. Because of these risks, agencies must start business continuity and contingency planning now in order to reduce the risk of Year 2000-induced business failures.

Interior has recognized, to some degree, the critical need for contingency planning, and has asked its bureaus and offices to develop such plans for all mission-critical systems that are behind schedule. However, it has not instructed its component organizations to develop plans to ensure the continuity of core business operations. As noted, agencies developing such plans only for systems currently behind schedule 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 Year 2000-induced failures of internal information systems.

In conclusion, the change of century will initially present many difficult challenges in information technology and continuity of business operations, and has the potential to cause serious disruption to the nation and to the Department of the Interior. These risks can be mitigated and disruptions minimized with proper attention and management. While Interior has been working to mitigate its Year 2000 risks, further action must be taken to avoid losing the ability to continue mission-critical business operations. Continued congressional oversight through hearings

such as this can help ensure that such attention continues and that appropriate actions are taken to address this crisis.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Committee 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 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).

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

Official Business
Penalty for Private Use $300

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100