United States General Accounting Office

GAO

Testimony

Before the Committee on Banking and Financial Services, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
September 17, 1998

YEAR 2000 COMPUTING CRISIS

Federal Depository Institution Regulators Are Making Progress, But Challenges Remain

Statement of Jack L. Brock, Jr.,
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

GAO/T-AIMD-98-305

Mr. Chairman and Members of the Committee:

I am pleased to be here to discuss the progress of the federal regulatory agencies in ensuring that the thousands of financial institutions[1] they oversee are ready for the upcoming century date change. As you know, banks, thrifts, and credit unions are extremely vulnerable to Year 2000 problems due to their widespread dependence on computer systems to make loans, invest deposits, transfer funds, issue credit cards, and handle routine business functions, such as accounting and personnel management. At the very least, Year 2000 problems[2] could cause significant inconveniences to financial institutions and their customers. More significantly, system failures could lead to closings and serious disruptions to payment systems and credit flows. Today, I will discuss the Year 2000 risks facing financial institutions and the federal regulators, highlight actions taken to date to mitigate these risks, and address the challenges ahead as institutions and regulators face the more complex and difficult activities of their Year 2000 programs.

This testimony is one in a series of reports and testimonies that we have issued at this Committee's request on the status of efforts by the five federal financial regulatory agencies to ensure that the institutions they oversee are ready to handle the Year 2000 computer conversion challenge. We previously reported on the status of the National Credit Union Administration (NCUA), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS).[3] Today, we are also reporting on the Federal Reserve System's (FRS) efforts to oversee the Year 2000 progress of the institutions it supervises.[4] This statement incorporates the

[1]In this report, financial institutions refers to commercial banks, thrifts, and credit unions.

[2]The Year 2000 problem is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900, or 2001 from 1901. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results.

[3]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); Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 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: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998); FDIC's Year 2000 Preparedness (GAO/AIMD-98-108R, March 18, 1998); and Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998).

[4]Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems, But Challenges Remain (GAO/AIMD-98-248, September 17, 1998).

results of that review as well as our recently completed review of the Office of the Comptroller of the Currency (OCC). We plan to conclude this series with a report on the FRS' internal system conversion efforts in the coming months. Therefore, my statement today excludes any discussion of that ongoing review.

To prepare for this testimony, we evaluated regulator efforts to date to ensure that the institutions they oversee are adequately mitigating the risks associated with the Year 2000 date change. We compared their efforts to criteria detailed in our Year 2000 Assessment Guide,[5] Business Continuity and Contingency Planning Guide,[6] and Testing Guide[7] as well as Year 2000 examination guidance and procedures set forth by the Federal Financial Institutions Examination Council (FFIEC).[8] We reviewed procedures and guidance developed by the regulators to perform their industry assessments. We also reviewed regulator reports to the Congress on the status of their efforts to correct internal systems and to oversee financial institution Year 2000 readiness. We reviewed relevant correspondence from the regulators to their examiners and the institutions they supervise and interviewed officials responsible for overseeing the safety and soundness of financial institution management practices and procedures. We also interviewed officials from various trade associations representing banks, thrifts, and credit unions to obtain their views on the adequacy of regulatory efforts and determine what the bank, thrift, and credit union communities were doing to ensure Year 2000 readiness.

[5]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14). Published as an exposure draft in February 1997 and finalized in September 1997, the guide was issued to help federal agencies prepare for the Year 2000 conversion. It advocates a structured approach to planning and managing an effective Year 2000 program through five phases: (1) raising awareness of the problem, (2) assessing the extent and severity of the problem and identifying and prioritizing remediation efforts, (3) renovating, or correcting, systems, (4) validating, or testing, corrections, and (5) implementing corrected systems.

[6]Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19). Published as an exposure draft in March 1998 and finalized in August 1998, this guide provides a conceptual framework for helping organizations to manage the risk of potential Year 2000-induced disruptions to their operations. It discusses the scope and challenge and offers a structured approach for reviewing the adequacy of agency Year 2000 business continuity and contingency planning efforts.

[7]Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, Exposure Draft, June 1998). This guide addresses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion. The guide describes a step-by-step framework for managing, and a checklist for assessing, all Year 2000 testing activities, including those activities associated with computer systems or system components (such as embedded processors) that are vendor supported.

[8]FFIEC was established in 1979 as a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions, and to make recommendations to promote uniformity in the supervision of these institutions. The Council's membership is composed of the federal financial institution regulators—FDIC, FRS, OCC, OTS, and NCUA.

Information on Year 2000 readiness of internal regulator systems and the status of institutions was provided by the regulators and was not independently verified by us. Our work was performed at the regulators between October 1997 and September 1998 in accordance with generally accepted government auditing standards.

In summary, we found that the regulators have made good progress in assisting banks, thrifts, and credit unions in their Year 2000 efforts as well as identifying which institutions are at a high risk of not remediating their systems on time. They have also recognized the risk and potential impact of Year 2000-induced system failures on their own core business processes and have implemented rigorous efforts to mitigate these risks.

Nevertheless, there are still serious challenges ahead that could threaten the financial institution industry's ability to successfully meet the Year 2000 deadline.

- First, there is the challenge of time. With less than 16 months remaining before the Year 2000 deadline, the regulators are faced with the daunting task of overseeing the efforts of more than 22,000 financial institutions, service providers, and software vendors with a relatively finite number of examination personnel.
- Second, in the next few months, many of these entities will be undertaking the most complex and difficult stage of correction—testing. It will be necessary for regulators to ensure that they have enough technical resources to review institution efforts during this crucial phase.
- Third, beginning in early 1999, regulators will be pressed to take quick actions against institutions that cannot successfully complete their Year 2000 efforts. But before they can do so, they need to determine what will constitute financial institution Year 2000 failures, what regulatory options can be effectively used, and when they would be implemented.
- Fourth, the U.S. economy is intrinsically linked to the international banking and financial services sector, yet many countries and their financial institutions are reported to be behind schedule in addressing their Year 2000 problem. Working with their foreign counterparts, the regulators will need to identify and define global Year 2000 risks and work cooperatively to mitigate those risks. The regulators will also need to develop contingency plans in case there are unforeseen problems.
- Fifth, financial institution credit, deposit, and payment flows are critically dependent on public infrastructure, such as telecommunications and electric power networks; however, until critical readiness assessments and tests are completed and made available to the public, it is not clear

whether there will be uninterrupted telecommunications and power service. Again, regulators will need to develop contingency plans that anticipate Year 2000-related disruptions in the public infrastructure.

Background

The federal financial regulators are responsible for examining and monitoring the safety and soundness of approximately 22,000 financial institutions, which, together, manage more than $13 trillion in assets and hold over $7 trillion in deposits. Specifically:

- The Federal Reserve System is responsible for overseeing the Year 2000 activities of 1,618 entities, including 990 state member banks, 349 bank holding companies, 221 foreign bank offices, and 9 Edge Act corporations.[9] According to FRS, these organizations have assets totaling over $7.7 trillion and hold deposits of about $3.6 trillion. FRS' oversight responsibilities also include 49 service providers, software vendors, and data centers.
- The Office of the Comptroller of the Currency supervises about 2,600 federally-chartered, national banks and federal branches and agencies of foreign banks, which comprise about $3.5 trillion in assets. OCC is also responsible for monitoring the Year 2000 activities of 109 service providers, software vendors, and data centers.
- The Federal Deposit Insurance Corporation supervises about 6,000 state-chartered, nonmember banks, which are responsible for about $1 trillion in assets. It is also the deposit insurer of approximately 11,000 banks and savings institutions that have insured deposits totaling upwards of $3.8 trillion. FDIC also oversees 146 service providers, software vendors, and data centers.
- The Office of Thrift Supervision oversees about 1,200 savings and loan associations (thrifts), which primarily emphasize residential mortgage lending and are an important source of housing credit. These institutions hold approximately $737 billion in assets.
- The National Credit Union Administration supervises about 7,000 federally-chartered credit unions. It is also the deposit insurer of more than 11,000 federally- and state-chartered credit unions whose assets total about $371 billion. Credit unions are nonprofit financial cooperatives organized to provide their members with low-cost financial services.

As part of their goal of maintaining safety and soundness, these regulators are responsible for assessing whether the institutions they supervise are adequately mitigating the risks associated with the century date change.

[9]Edge Act corporations are corporations chartered by FRS to engage in international banking. The Board of Governors of FRS reviews and approves the applications to establish Edge Act corporations and also has supervisory responsibility for examining the corporations and their subsidiaries.

To ensure consistent and uniform supervision on the Year 2000 issue, the five regulators are coordinating their supervisory efforts through FFIEC. Additionally, under the auspices of the FFIEC, the regulators are jointly examining 28 major data service providers and software vendors that support the financial institutions. Each of the regulators, except NCUA, is responsible for a specified number of these joint examinations.

Year 2000 Risks Confronting Financial Institutions and Regulators

Addressing the Year 2000 problem in time has been, and will continue to be, a tremendous challenge for financial institutions and their regulators. Virtually every insured financial institution relies on computers—either their own or those of a contractor—to process and update records and for a variety of other functions. To complicate matters, most institutions have computer systems that interface with systems belonging to payment systems partners, such as wire transfer systems, automated clearinghouses, check clearing providers, credit card merchant and issuing systems, automated teller machine (ATM) networks, electronic data interchange systems, and electronic benefits transfer systems. Because of these interdependencies, financial institutions systems are also vulnerable to failure caused by incorrectly formatted data provided by other systems that are not Year 2000 compliant.

In addition, financial institutions depend on public infrastructure, such as telecommunications and power networks, to carry out critical business operations, such as making electronic fund transfers, verifying credit card transactions, and making ATM transactions. However, these networks are also susceptible to Year 2000 problems. Thus, financial institutions must also assess the Year 2000 readiness efforts of their local utilities and telecommunications providers.

Financial institutions and their regulators cannot afford to neglect any of these issues. If they do, the impact of Year 2000 failures could be potentially disruptive to vital bank operations and harmful to customers. For example, loan systems could make errors in calculating interest and amortization schedules. In turn, these miscalculations may expose institutions and data centers to financial liability and loss of customer confidence. Moreover, ATMs may malfunction, performing erroneous transactions or refusing to process transactions. Other supporting systems critical to the day-to-day business of financial institutions may be affected as well. For example, telephone systems, vaults, and security and alarm systems could malfunction.

Regulators Have Taken Positive Actions to Mitigate Year 2000 Risks

Since June 1996, when their Year 2000 oversight efforts began, the five financial institution regulators have taken a number of important steps to alert financial institutions of the risks associated with the Year 2000 problem and to assess what these institutions are doing to mitigate the risks. To raise awareness, the regulators issued letters to financial institutions that described the Year 2000 problem and special risks facing financial institutions and recommended approaches to planning and managing effective Year 2000 programs. In addition, the regulators provided extensive guidance to assist financial institutions in critical Year 2000 tasks, including guidance on (1) contingency planning, (2) mitigating risks associated with critical bank customers (e.g., large borrowers and capital providers), (3) mitigating risks of using data processing servicers and software vendors to perform financial institution operations, (4) testing to demonstrate Year 2000 compliance, (5) establishing effective Year 2000 customer awareness programs, and (6) addressing Year 2000 risks associated with fiduciary services. The regulators have also undertaken extensive outreach efforts—such as establishing Internet sites and conducting seminars nationwide—to raise the Year 2000 awareness of banking industry personnel and the public.

To assess what institutions are doing to mitigate Year 2000 risks, the regulators performed a high-level and detailed assessment of bank, thrift, and credit union efforts. The high-level assessment consisted primarily of administering FFIEC's Year 2000 questionnaire via telephone and on-site visits and was completed during November and December 1997. During this assessment, the regulators examined whether institutions had established a structured process for correcting the problem; estimated the costs of remediation; prioritized systems for correction; and determined the Year 2000 impact on other internal systems important to day-to-day operations, such as vaults, security and alarm systems, elevators, and telephones. The more detailed Year 2000 assessment involved on-site visits to the institutions and was completed in June 1998. These examinations focused on whether institutions were appropriately planning for the Year 2000 effort and addressing risks posed by service providers, software vendors, and large customers. They also began to assess whether institutions had effective customer awareness programs.

These exams found the majority of financial institutions are doing an adequate job in addressing the Year 2000 issue. Specifically, according to the regulators, they found that of the over 22,000 institutions with examinations completed by June 30, 1998, almost 93 percent were doing a

satisfactory job of addressing their Year 2000 problems, about 7 percent needed improvement, and 0.3 percent were performing unsatisfactorily.

The regulators plan to follow up with additional on-site visits that will address the unique—and more difficult—challenges that the testing and implementation phases will present. These exams, which the regulators plan to complete by March 31, 1999, are expected to identify institutions that are experiencing difficulties completing their testing and implementation programs or have not developed sufficient contingency plans.

Regulators Have Also Taken Positive Steps to Remediate Internal Systems

In addition to overseeing the efforts of financial institutions to address the Year 2000 problem, the federal regulators must also ensure that their internal computer systems are Year 2000 compliant. This is especially critical for FRS which operates systems on which the financial institutions heavily rely. For example, according to FRS, the Fedwire system was used by financial institutions in 1997 to make about 89 million funds transfers valued at $288 trillion. While systems belonging to the other regulators are not critical to the day-to-day operation of the banking industry, they support the essential business functions of the regulators, such as personnel management, accounting, budget, travel, and program tracking.

As noted earlier, we are currently reviewing FRS' efforts to remediate its internal systems and plan to report the results of our review separately. However, we have reviewed the efforts of the four other regulators to remediate their systems and found that they have taken many actions that are crucial to successfully dealing with the Year 2000 problem. For example, they have established a good foundation for managing their remediation efforts by developing Year 2000 strategies, designating Year 2000 program managers, inventorying systems, and developing tracking systems to monitor progress and prepare status reports. They are acting or have acted to ensure that core business operations are not disrupted by identifying core business operations, assessing the potential impact of Year 2000-induced failures (including public infrastructure failures) on those operations, prioritizing conversion efforts, and developing contingency plans. The regulators also have identified their data exchanges and are working with their data exchange partners to prevent noncompliant systems from introducing Year 2000 errors into compliant systems. Finally, to ensure that their systems are adequately tested, the regulators have developed Year 2000 testing guidance and have begun or are well underway in testing their systems.

In September 1998, each of the regulators reported to the Congress that they are on schedule to meet the Office of Management and Budget's March 1999 implementation date for their mission-critical systems. Their data indicate that, with continued good management, the regulators should be able to meet this milestone.

Regulators Have Responded Quickly to GAO Findings and Recommendations

While the regulators have been working hard to achieve industrywide compliance and remediate their own systems, we have identified concerns and problems with their efforts during the course of our reviews. Specifically, we found that all the regulators were late in initiating their Year 2000 oversight of institutions and in issuing key guidance on business continuity and contingency planning, corporate borrowers, and service providers and software vendors. We also found that the regulators had not assessed whether they had enough information system examiners to adequately oversee the Year 2000 efforts of the institutions they supervise. In addition to these general concerns, we also found problems specific to each agency.

However, the regulators have been quick to respond to our recommendations and to implement corrective actions. For example, in October 1997, we made recommendations to NCUA to help it ensure that credit unions were adequately mitigating Year 2000 risks. Among other things, NCUA responded by (1) implementing a quarterly reporting process whereby credit unions would communicate the status of their remediation efforts between examinations, (2) developing a formal, detailed plan for contingencies, (3) instructing credit union management to have their auditors address Year 2000 issues in the scope of their work, and (4) hiring additional contractor support to assist with exams of credit unions and service providers. We also made specific recommendations to FDIC to (1) work with the other FFIEC members to enhance the content of their assessment work program, (2) ensure that adequate resources are allocated to complete the corporation's internal systems' assessment by the end of March 1998, and (3) develop contingency plans for each of FDIC's mission-critical systems and core business processes. Similarly, we recommended that OTS develop contingency plans for each of its mission-critical systems and core business processes. Again, both agencies agreed with our recommendations and took immediate steps to implement them.

Significant Year 2000 Challenges Ahead for Financial Institutions and Regulators

Despite the regulators' strong efforts to assess industrywide compliance and remediate their own systems, several complex and difficult challenges remain in achieving Year 2000 compliance.

First: the challenge of time. Regardless of good practices and good progress, less than 16 months remain to the century date change. With over 22,000 institutions, vendors, and service providers to examine and monitor, the regulators face a formidable task in continuing to provide adequate coverage.

Second: the challenge to provide effective oversight during the later and more complicated stages of the remediation effort. By December 1998, FFIEC expects financial institutions to be well into the testing phase. As noted in our Year 2000 Test Guide, because Year 2000 conversions often involve numerous, large interconnecting systems with many external interfaces and extensive supporting technology infrastructures, testing needs to be approached in a structured and disciplined fashion. According to OCC, for many banks, testing will consume upwards of 60 percent of the cost and time spent to correct Year 2000 problems. Nevertheless, the regulators have a small window of opportunity for assessing institutions during this critical phase: they generally expect to complete on-site exams of service providers, software vendors, and institutions with in-house or complex systems by December 31, 1998, and plan to complete on-site exams for the remaining institutions by March 31, 1999. At the same time, however, they have a limited number of technical examiners to conduct these reviews. OCC, for example, has 79 full-time bank information system examiners responsible for providing assistance to 575 safety and soundness examiners and for examining institutions with complex systems. FRS currently has 73 such examiners—31 full time and 42 part time—that conduct complex examinations while supporting 106 other examiners during their exams. Because of the limited number of technical examiners and the large number of entities to be examined, we have recommended to the regulators that they (1) determine how many technical examiners are needed to adequately oversee the Year 2000 efforts of the institutions, data processing servicers, and software vendors and (2) develop a strategy for obtaining these resources and maintaining their availability.

Third: the challenge to develop an effective strategy for dealing with institutions that by all indications will not be viable by the Year 2000. The regulators have not yet (1) defined the criteria for finding that a financial institution will not be viable due to Year 2000 problems or (2) developed a

strategy for when and how they will handle such troubled institutions. The regulators have been working on these issues. For example, they are querying data centers and service providers on their capacity to service new clients due to Year 2000 problems and putting together a "bidders list" for Year 2000 purposes that will include institutions that have demonstrated, well-managed Year 2000 programs and are capable of processing acquisitions of other institutions. However, none of these efforts have been finalized. Developing these plans promptly is paramount to minimizing the risk of not having enough time to implement a viable plan for dealing with institutions that cannot successfully complete their efforts.

Fourth: the challenge to protect U.S. banks from international Year 2000 risks. U.S. banks have many external links to financial institutions and markets around the world. For example, overseas financial institutions and markets depend on our electronic funds transfer systems and clearinghouses. Unfortunately, it has been reported that many countries are well behind their U.S. counterparts in Year 2000 remediation. For example, a survey of 15,000 companies in 87 countries by the Gartner Group found that nations including Germany, India, Japan, and Russia were 12 months or more behind the United States.[10] Given the fact that many countries are behind schedule in addressing the Year 2000 problem, it will be essential for regulators to (1) ensure that financial institutions have adequately identified and mitigated their international risks and (2) prepare contingency plans for handling disruptions caused by problems abroad.

Fifth: the challenge to protect financial institutions from Year 2000 disruptions caused by their telecommunications and power service providers. The most vital business operations of financial institutions—ATM transactions, fund transfers, and credit card authorizations, for example—are dependent on telecommunications and power networks. In fact, according to the President's National Security Telecommunications Advisory Committee, the financial services industry may be the telecommunications industry's most demanding customer: over $2 trillion is sent by international wire transfers every day.

In June 1998 testimony on the Year 2000 readiness of the telecommunications sector, we reported that most major telecommunications carriers expect to achieve Year 2000 network

[10]Year 2000 World Status 2Q98 Update - A Summary Report (Gartner Group, Report #M-04-6957, July 21, 1998).

compliance by December 1998. For a few though, the planned date for compliance is either later than December 1998, or we were unable to obtain this information.[11] The carriers are working to test their networks but until the tests are completed and the results made public, it is not clear to what degree—if any—financial institutions and the public will be subject to telecommunications disruptions.

The situation for electric power companies is similar. At the request of the Department of Energy, the North American Electric Reliability Council (NERC) is assessing the readiness of the critical systems within the nation's electric infrastructure. The Secretary of Energy requested that NERC provide written assurances by July 1, 1999, that critical power systems have been tested, and that such systems will be ready to operate in the year 2000. Until such assessments are completed and results made public, the precise status of this sector is not completely clear. Because of the uncertain nature of electric power and telecommunications Year 2000 readiness, it is essential for regulators and institutions to plan for contingencies should there be service disruptions due to the Year 2000 date change.

In conclusion, the regulators have made significant progress in assessing the readiness of member institutions; raising awareness on important issues such as contingency planning, testing, and dealing with service providers, software vendors, and large customers; and remediating their own systems. Looking forward, the challenge is for the regulators to make the best use of limited resources in the time remaining and to ensure that they are ready to take swift actions to address those institutions that falter in the later phases of correction and to address disruptions caused by international and public infrastructure Year 2000 failures. To their credit, the regulators have spent the last year developing a picture of how their industry stands, including which institutions are at high risk of not being ready for the millennium and require immediate attention, which service providers and vendors are likely to be problematic, and the extent of problems remaining. In addition, they have undertaken efforts to determine what conditions will constitute Year 2000 failures and what actions can be taken to quickly address failures. Nevertheless, more needs to be done to prepare for major potential disruptions caused by domestic and international financial institutions, as well as power and

[11]Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June, 16, 1998).

telecommunications companies, experiencing processing problems at the century date rollover.

Accordingly, we are now recommending that the regulators, working through the FFIEC, (1) finalize by December 1, 1998, their plans for dealing with institutions that will be not be viable due to Year 2000 problems and (2) develop contingency plans that address international and public infrastructure Year 2000 risks.

Mr. Chairman, this concludes my statement. We welcome any questions that you or Members of the Committee may have.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

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