United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EDT
on Tuesday
August 3, 1999

ELECTRONIC BANKING

Enhancing Federal Oversight of Internet Banking Activities

Statement of Richard J. Hillman, Associate Director
Financial Institutions and Markets Issues
General Government Division

GAO/T-GGD-99-152

Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss regulatory efforts to identify and mitigate risks to U.S. depository institutions' operations introduced by the growth in the use of Internet banking systems. This testimony summarizes the findings in our July 6, 1999,[1] report, which responded to the Committee on Banking and Financial Services' request asking us to

- describe risks posed by Internet banking and the extent of any industrywide Internet banking problems,
- assess how the five U.S. financial regulators track institutions' plans to provide Internet banking services,
- determine how regulators have begun to examine Internet banking activities, and
- determine the extent to which regulators have examined firms providing Internet banking support services to institutions.

To summarize our findings, I will highlight four main points that emerged from our work.

First, we found that Internet banking heightens various types of traditional banking risks and our review of 81 examinations showed that roughly 44 percent of the depository institutions examined had not completely implemented risk-management steps that regulators said are needed to limit on-line banking risks. Shortcomings included some institutions' lack of approval of strategic plans by their board of directors and a lack of policies and procedures at some institutions for Internet banking operations. However, I need to point out that too few examinations had been conducted at the time of our review to identify the extent of any industrywide Internet banking-related problems. Regulators attributed their limited number of examinations to a diversion of examiners to higher-priority efforts to address the Year 2000 computer problems and to their limited number of examiners with expertise in information systems.[2]

Second, our work found that some regulators could use more systematic methods for identifying institutions' plans for new Internet banking

[1] See Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities (GAO/GGD-99-91, July 6, 1999).

[2] The Year 2000 computer problem exists because the data that computers store and process often use only the last two digits to designate the year. On January 1, 2000, such systems may mistake data referring to 2000 as meaning 1900, possibly leading to errors and disruptions in the processing of financial data.

systems and maintaining this information centrally. We found that regulators use a variety of methods to identify depository institutions that already offer Internet banking services, but that only two of the regulators centrally collected information on plans for new services. The Office of Thrift Supervision (OTS) requires institutions to notify it in advance of their plans to establish a transactional Web site. Also, the Federal Deposit Insurance Corporation (FDIC) requires its examiners to keep abreast of institutions' plans to start offering Internet banking service**,** and it maintains records of these plans in a central database. We found that the other regulators could benefit from adopting systems to keep abreast of institutions' plans for new Internet banking services and to allow them to proactively oversee this new and evolving banking activity.

Third, we found variations in the supervisory approaches the regulators followed to help ensure that institutions mitigate the risks posed by Internet banking. As I will discuss in greater detail later, some regulators have been more proactive than others. We found that FDIC has completed the most examinations of on-line banking operations, and that OTS and FDIC have been actively issuing policies and procedures for Internet banking examinations. In contrast, the National Credit Union Administration (NCUA) had not conducted any Internet banking examinations at the time of our fieldwork and was the only regulator that had not developed procedures for Internet banking examinations.

In a fourth area, involving another critical oversight responsibility, we found that the five regulators are beginning to work cooperatively to carry out a study of third-party firms providing Internet banking support services. Such a joint study can enable regulators to share scarce technical resources on issues of mutual interest. The study is expected to provide the regulators with a greater understanding of the kinds of services and security features provided to institutions by third-party firms. In addition, the study should allow regulators to determine what form of additional oversight is necessary. Although NCUA is part of the joint study, we are concerned that third-party firms providing services solely to credit unions are not being reviewed. In addition, we are concerned that NCUA's authority to oversee these firms will sunset in December 2001.[3]

Information discussed in our report was gathered from reviews of examinations and interviews we had with officials from the five financial regulators on Internet banking risks and their strategies for overseeing

[3] The Examination Parity and Year 2000 Readiness for Financial Institutions Act, P.L. 105-162, 112 Stat. 32 (1998).

Internet banking activities. We also determined how these regulators identify institutions offering Internet banking, how they conduct safety and soundness and information systems examinations for Internet banking, and what approaches they used to examine third-party firms that provide Internet banking services. We also talked to a number of representatives from selected depository institutions and third-party firms about their views on the scope and frequency of regulators' examinations and their views of risks posed by Internet banking. As a key part of our work, we also reviewed 81 safety and soundness and information systems examinations that looked at on-line banking operations, and we interviewed 43 examiners who had conducted the examinations. We did this work between April 1998 and May 1999 in accordance with generally accepted government auditing standards.

Internet Banking Heightens Risks that Challenge Regulators

To elaborate on the findings in our report, I want to start by discussing growth in Internet banking and the kind of risks it presents. For the most part, regulators have taken steps to provide guidance to depository institutions on the need to mitigate risks. However, in some areas, more remains to be done.

Internet Banking Growth Continues

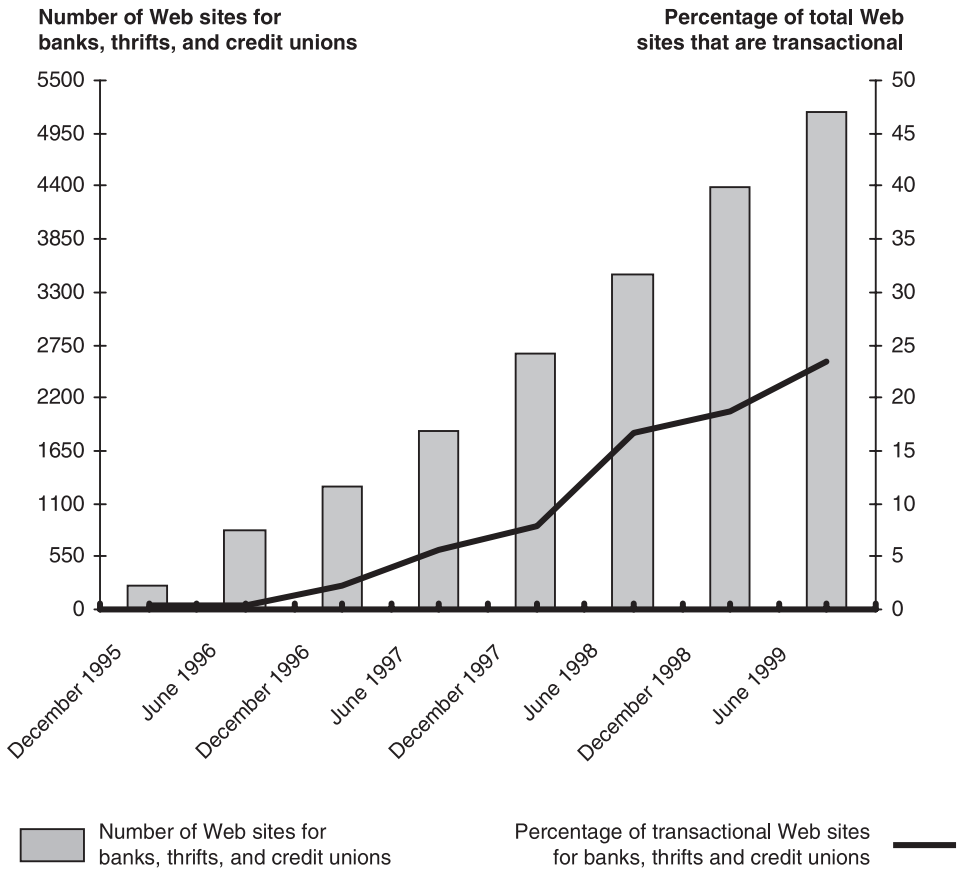
Internet banking services are offered by a fast growing number of depository institutions. When we concluded our fieldwork several months ago, about 3,600 federally insured depository institutions—or about 17 percent of all U.S. banks, thrifts, and credit unions—offered some form of Internet banking service.[4] More recent data showed that over 5,100 federally insured depository institutions, or about 24 percent, offered some form of Internet banking.[5] About a fourth of these institutions offered fully transactional Web sites.[6] It's important to differentiate these transactional sites - - which offer a range of interactive banking services, such as transferring of funds among customer accounts - - from Web sites that only give information about the bank and its services. As shown in figure 1, the most recent statistics showed that the number of banks, thrifts, and credit unions with Web sites has increased dramatically from 245 in December 1995 to over 5,100. Also, the number of banking Web sites that were transactional were growing as well from 1 in 1995 to over 1,200.

[4] In February 1999, approximately 2,500 banks and thrifts—about 23 percent of all banks and thrifts—had Web sites, according to FDIC. As of June 30, 1998, 1,110 credit unions had Web sites, according to NCUA.

[5] As of June 1999, approximately 3,000 banks and thrifts—about 30 percent of all banks and thrifts—had Web sites, according to FDIC. As of March 1999, 2,174 credit unions had Web sites, according to Callahan and Associates.

[6] According to FDIC, 635 banks and thrifts offered fully transactional Web sites as of June 30, 1999. According to Callahan and Associates, 578 credit unions offered such sites as of March 1999.

Figure 1: Growth in Internet Banking



Note: Credit union data was only available for June 1997 to March 1999.

Source: Bank and thrift data are from FDIC, and credit union data are from Callahan and Associates.

Projections suggest that households using Internet banking systems will increase from 6.6 million at the end of 1998 to 32 million by 2003.[7] This anticipated fast-paced growth makes it crucial that depository institutions and regulators understand various types of Internet banking risks and that institutions with these systems have procedures in place to mitigate these risks.

Regulators Need to Ensure Institutions Mitigate Risks

An underlying cause for the regulators' concerns in this area has been that many traditional banking risks are heightened by the access the Internet provides to anyone with a compatible computer and the resulting potential vulnerability to security breaches. We reviewed the guidance that

[7] Household projections developed by International Data Corporation.

regulators have provided to depository institutions, concerning various types of Internet banking risks, including security risk, transactional risk, and various types of strategic risk. Regulators are also concerned about risks associated with an institution's reputation, such as a possible loss of public confidence in an institution or the banking system caused by, for example, an Internet banking systems failure that prevents customers from accessing their accounts.

Our work assessing what regulators are doing to help ensure that institutions with on-line systems mitigate risks follows our earlier report[8] issued in 1998. In that report, we discussed information obtained from 93 banks about what they were doing to mitigate risks arising from their on-line and Internet banking services. An important step in ensuring the integrity of an on-line banking system is identifying vulnerabilities and threats potentially affecting individual on-line banking systems and establishing internal controls to mitigate these risks. Survey results discussed in our 1998 report indicated that 42 percent of the surveyed banks had not conducted formal risk assessments or did not know if they had performed one.

Since our 1998 report, we have found that the regulators issued varying amounts of guidance on how institutions can prepare for and mitigate risks, and we found that the limited number of examinations done so far have shown that many, but not all, institutions followed this guidance.

Limited Examinations Do Not Indicate the Extent of Any Industrywide Problems

Before I go into what we found in looking at examinations, I need to point out that, we found too few examinations had been completed to identify the extent of any industrywide Internet banking-related problems.[9] Reasons the regulators gave for the small number of examinations done to date included examiners being diverted to mitigation efforts concerning the Year 2000 computer problem and a shortage of trained examiners to carry out Internet banking examinations. I also want to point out that while examiners found deficiencies, none of the examinations we reviewed reported any financial losses or security breaches.

In the 81 depository institution examinations we reviewed, regulators found that 36, or about 44 percent, of those institutions had not completely

[8] Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking (GAO/GGD-98-34, Jan. 15, 1998).

[9] The examinations we reviewed included 62 that were conducted by FDIC, 6 by the Federal Reserve System(FRS), 8 by the Office of the Comptroller of the Currency (OCC), and 5 by the Office of Thrift Supervision (OTS).

implemented the on-line banking risk mitigation steps outlined by the regulator. These instances involved institutions' failure to implement, among other things, (1) active board and senior management oversight, (2) effective internal controls, and (3) comprehensive and ongoing internal audit programs.

As summarized in table 1, in 20 of the 81 examinations, or 25 percent of them, examiners discovered strategic planning deficiencies. For example, regulators found that some institutions had not prepared strategic plans or had not obtained board of directors' approval before initiating on-line banking. In 26 of the examinations, or 32 percent, regulators found that the institution did not have policies and procedures in place to guide its on-line banking operations.

Table 1: On-line Banking-Related Weaknesses in Risk Mitigation Systems

Type of weaknesses	Number of banks and thrifts	Percent of 81 institutions reviewed
Deficiencies in strategic planning	20	25%
No policies and procedures to address security concerns and standard operating practices	26	32
Insufficient audit coverage of on-line banking activities	29	36
Management had not properly initiated or documented agreements with third-party firms	15	18%

Source: GAO analysis of FDIC, FRS, OCC, and OTS data.

Another weakness involved institutions' audit coverage of their on-line banking operations. In 29 of the examinations, or 36 percent of them, regulators found that the institution lacked adequate audit coverage of its on-line banking operations. Fifteen examinations, or 18 percent of the ones we reviewed, disclosed that the institution had not taken steps to evaluate its third-party firm that was providing the on-line banking services or lacked a written contract with their firm. Examiners we interviewed expressed concerns about deficiencies that were similar to those we found in the examinations we reviewed. For example, examiners were concerned that some smaller institutions were implementing Internet banking systems before they had established operating policies and procedures and that bank management had to be reminded that operating policies and procedures were not optional.

Regulators Need to Share Examination Results to Benefit From Each Other's Experiences

As I noted earlier, too few examinations had been done at the time of our review to draw conclusions about patterns of problems emerging in the industry, and we are not able to generalize from the results of our review of these examinations. At the same time, we believe that as they continue to examine Internet banking, the regulators can and should learn from these examinations; and we believe that they need to begin sharing the results of their Internet banking examinations with each other.

As more examinations are completed, information sharing among the regulators could help them better understand the extent of the risks posed by Internet banking, develop risk profiles that would allow them to target institutions requiring further attention, and help them allocate limited resources among competing priorities.

Some Regulators Do Not Identify New Internet Banking Systems Plans

Before discussing how regulators supervise Internet banking, I want to touch on a problem we found in how some regulators identify depository institutions planning new Internet banking services.

We found that regulators used a variety of methods to identify institutions that were already offering Internet banking services, such as Internet Web site searches and examiners' preexamination planning information gathering. However, we found that only two regulators were systematically obtaining information on institutions' plans to provide such services and had a centralized database of this information at the time of our review. One of them, OTS, recently established a requirement that institutions notify it in advance of plans to establish a transactional Web site. The agency estimated that it would take an institution about 2 hours to prepare the notification, which in its judgment represented a minimal burden. OTS maintains this information in a centralized electronic database.

The other institution, FDIC, similarly gathers information on institutions' plans, but it relies on requirements it places on its examiners rather than placing them on the institutions it supervises. For instance, we found that during examinations of institutions not offering Internet banking, FDIC requires its examiners to find out whether the institution plans to establish Internet banking. Like OTS, FDIC collects this information in a central database.

With the number of institutions offering Internet banking services significantly increasing, it is critically important for the regulators to stay abreast of which institutions are beginning to offer new Internet banking services—both to head off problems and to be able to furnish guidance to institutions at an early point when they are still installing and fine-tuning

their systems. Methods, such as those used by OTS and FDIC, could be used by the other regulators to inform them about Internet banking plans and activities and better enable them to provide tailored risk-management guidance to individual depository institutions when needed. Regulators could also use this information to plan the scope and timing of future examinations and to determine the need for additional examiners who have information technology expertise.

Regulators' Approaches to Internet Banking Supervision Vary

During our review, most regulators were developing, testing, or implementing new on-line banking examination procedures, including procedures for examinations of Internet banking. However, their approaches varied on whether (1) examinations of new Internet banking activities were required or discretionary and, (2) safety and soundness examiners or information system examiners conducted the examinations. The regulators also varied in their approaches to training.

Regulators' Efforts to Supervise New Internet Banking Systems Differ

We found that regulators' policies differed in the discretion examiners had to decide whether to examine an institution's new Internet banking activity. FDIC and OTS expected their examiners to review an institution's Internet banking activities during the first examination of the institution after it has gone on-line. FRS and OCC, in contrast, did not require that an institution's new Internet banking activities be examined. They permitted their examiners to determine whether they should examine an institution's new Internet banking activity. They reasoned that although Internet banking is an evolving activity that may warrant scrutiny, its small size, relative to an institution's overall assets in most cases does not present a safety and soundness concern to the bank; and therefore, examinations of new Internet banking activities are considered optional for their examiners.

We found that NCUA was the only regulator that had not established procedures for Internet banking examinations or conducted such examinations. NCUA officials explained that the agency had not conducted Internet banking examinations (1) because the number of NCUA examiners with expertise in information systems was limited and (2) because some examiners who might have been looking at credit unions' Internet banking services in the past 2 years had been diverted to higher-priority efforts concerning the Year 2000 computer problem. We concluded from our fieldwork that NCUA's lack of an Internet banking examination program meant it could not provide adequate assurances that credit unions with Internet banking were appropriately managing risks. This is particularly troublesome given concerns expressed by some that smaller institutions might be moving too quickly into Internet banking because of

the relatively low costs of providing such services through third-party firms and the desire to remain competitive.

In other areas, we found differences in the types of examiners assigned to Internet banking examinations. While FRS and FDIC predominantly relied on their safety and soundness examiners for examinations of Internet banking, two other regulators relied entirely or primarily on information systems specialists. OCC relied entirely on specialized examiners because it believed the technology-related aspects of Internet banking required their expertise. OTS relied primarily on information systems specialists for examinations of Internet banking services offered by complex or large institutions.

We also found that regulators were at different stages of training their examiners to carry out Internet banking examinations. At the time of our fieldwork, FDIC had largely completed its basic training for its safety and soundness examiners, but it planned additional training for subject matter experts. OTS told us that it would be finished training its examiners by the end of the year, and FRS said it also expected to complete an initial training program for its safety and soundness examiners by the end of this year. OCC had no plans for in-house training of its safety and soundness examiners in on-line banking examinations, because its on-line banking examinations are performed by information system specialists who receive specialized external training. At the time of our review, NCUA had not yet provided its examiners with special training on conducting examinations of Internet banking.

Third-Party Firms Providing Internet Banking Services Pose a Regulatory Challenge

The final area of our review involved regulatory oversight of third-party firms. These firms supply Internet banking support services under contract to many depository institutions which cannot or choose not to provide these services themselves. Each regulator has the authority to examine institutions' banking services provided by third-party firms. Laws enacted in 1962 and 1998 show that Congress intended that banking services outsourced to third-party firms should be subjected to the same level of supervisory attention as services provided by the banks themselves.[10] Over time, this authority to examine third-party firms has grown in importance, as institutions have contracted out an increasing proportion of their operations. However, our work indicated that regulators are in the early stages of determining their role in overseeing third-party firms that provide Internet banking services.

[10] The Bank Service Company Act, 12 U.S.C. 1861-1867 (1962), and the Examination Parity and Year 2000 Readiness for Financial Institutions Act, P.L. 105-162, 112 Stat. 32 (1998).

Joint Reviews By Regulators Could Enhance Oversight Of Third-Party Firms

We found that to avoid duplicating efforts, regulators often cooperated in reviewing third-party firms. Joint reviews of firms providing Internet banking services could enable regulators to share technical resources and fill gaps in their expertise. In late 1998, the five regulators, working under the auspices of the Federal Financial Institutions Examination Council (FFIEC), cooperatively initiated a joint study of Internet banking services provided by third-party firms. The study is expected to provide the regulators with a greater understanding of the services and security features provided to institutions by third-party firms. In addition, the study should allow regulators to determine what form of additional oversight is necessary.

In updating our information for this testimony, we were told that as part of the joint study, regulators have met with five of the largest third-party firms to discuss risks associated with Internet banking, to gain a better understanding of available products and services and the associated security features of those products and services, and to obtain information on these firms' contingency plans. A spokesperson for the study said that the group plans to summarize its findings in a report to FFIEC, and that it is considering issuing new guidance to its member regulators and to their examiners.

Sunsetting of NCUA Authority Hinders Oversight of Third-Party Firms

Before leaving the oversight of third-party firms, I want to mention a potential problem involving the pending expiration of NCUA's authority to examine third-party firms, and a matter that the Congress may wish to consider so as to ensure that NCUA has the authority it needs to maintain its oversight over third-party firms.

Although each regulator has the authority to examine third-party firms providing services to depository institutions, NCUA's authority to examine such firms expires in 17 months on December 31, 2001. According to the NCUA officials that we talked with, its authority originally was granted so that NCUA could conduct examinations related to the Year 2000 computer problem. At the time of our fieldwork NCUA had not examined any third-party firm's Internet banking services; but NCUA officials recognized the need to begin to conduct such examinations. However, the expiration of NCUA's authority to carry out these examinations on December 31, 2001, would seriously compromise NCUA's future ability to effectively oversee third-party firms. This is of particular concern because most credit unions offering Internet banking services lack the necessary in-house expertise and rely heavily on third-party firms to provide support services, according to NCUA officials.

NCUA staff have recently been discussing the agency's sunset provision contained in the Examination Parity and Year 2000 Readiness For Financial Institutions Act, and plan to request that Congress amend the provision to provide permanent supervisory authority over service providers.

Recommended Changes to Improve Internet Banking Supervision

In response to the concerns I have touched on, we raised a matter for congressional consideration and made a number of recommendations to banking regulators. In general, banking regulators concurred with the thrust of our findings, conclusions, and recommendations.

Matter for Congressional Consideration

Specifically, as a matter for congressional consideration, our report suggested that Congress may wish to consider whether NCUA's current authority to examine the performance of services provided to credit unions by third-party firms needs to be extended to ensure the safety and soundness of credit unions. As I noted earlier, NCUA also believes it needs to maintain its authority to examine third-party firms providing support services to credit unions.

Recommendations to Banking Regulators

In our report, we recommended that as regulators gain experience in examining Internet banking services, the heads of the banking regulatory agencies should share information on the problems institutions are having in their Internet banking operations. As part of this effort, we also recommended that the heads of the banking regulatory agencies share information on Internet banking examination methods that they find work best. The regulators concurred with this recommendation.

We recommended that the Comptroller of the Currency, the Chairman of the Board of Governors of the Federal Reserve System, and the Chairman of the National Credit Union Administration establish procedures to obtain more timely information on institutions' plans to offer Internet banking. We proposed that they use this information to (1) assess technological trends and emerging security and compliance issues, (2) provide timely and specific risk-management guidance to institutions, and (3) plan the scope and timing of future examinations as well as plan for the availability of examiners with appropriate information systems expertise. The three regulators generally agreed with the thrust of this recommendation and discussed ways to obtain more timely information.

To help ensure that reviews of the adequacy of Internet banking services provided by third-party firms are conducted in a cost-efficient manner, we

recommended that the Chairman of FFIEC, through the FFIEC Task Force on Supervision, develop plans and a timetable for the regulators' joint oversight of third-party firms. The regulators generally concurred with the need to develop supervisory plans, with respect to the outsourcing of Internet banking operations of depository institutions. However, FRS commented that it was not clear whether we were recommending a change in the regulators' current regulatory approach. We believe that joint regulatory examinations of the operations of third-party firms providing depository institutions' Internet banking services could lead to more economical and efficient oversight. In this regard, our recommendation is intended to ensure that an interagency strategy, instead of individual agency strategies, is developed to examine third-party firms.

Finally, we recommended that, as work related to the Year 2000 computer problem diminishes, the Chairman of NCUA expeditiously develop Internet banking examination procedures and begin to examine credit unions' Internet banking-related activities. NCUA agreed with this recommendation and expressed its intention to increase its efforts on Internet banking-related examinations. In this regard, we are hopeful that the agency's stated intention to examine Internet banking activities represents an important step towards providing assurances that institutions with Internet banking are appropriately managing risks that could affect their safety and soundness.

This concludes my prepared statement. If you or other members of the Committee have any questions, I will be pleased to answer them.

Contact and Acknowledgments

For future contacts regarding this testimony, please contact Richard J. Hillman at (202) 512-8678. Individuals making key contributions to this testimony included Gerhard Brostrom, Robert Pollard, Karen Tremba, and Kane Wong.

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.

Order 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 touch-tone 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 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