United States General Accounting Office

GAO

Report to the Chairman of the Board of Governors of the Federal Reserve System

September 1999

FEDERAL RESERVE BANKS

Areas for Improvement in Computer Controls

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-283496

September 15, 1999

The Honorable Alan Greenspan
Chairman
Board of Governors of the Federal Reserve System

Dear Mr. Chairman:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1998 financial statements, we reviewed the general and application computer controls over key financial systems maintained and operated by the Federal Reserve Banks (FRB) on behalf of the Department of the Treasury's Financial Management Service (FMS) and Bureau of the Public Debt (BPD). On August 13, 1999, we issued a "Limited Official Use" report to you detailing the results of our review. This excerpted version of the report for public release summarizes the vulnerabilities we identified and the recommendation we made.

This report discusses our follow-up on the status of FRBs' corrective actions to address vulnerabilities identified in our fiscal year 1997 audit and the results of our fiscal year 1998 tests of the effectiveness of general and application controls that support key FMS and BPD automated financial systems maintained and operated by the FRBs.

Overall, we found that the FRBs had implemented effective general and application controls. However, as discussed in this report, we identified vulnerabilities involving general and application computer controls that we did not consider as having a significant adverse impact on key FMS and BPD systems but nonetheless warrant FRB management's attention and action. While performing our work, we communicated detailed information regarding our findings to FRB management. This report provides an overall assessment of the FRBs' computer control vulnerabilities and summarizes those findings.

Results in Brief

Our follow-up on the status of the FRBs' corrective actions to address vulnerabilities identified in our fiscal year 1997 audit found that the FRBs had corrected or mitigated the risks associated with 14 of the 20 general and application control vulnerabilities discussed in our prior report that related to the FRBs visited during our fiscal year 1998 testing.[1]

While we found that the FRBs had implemented effective general and application controls, our fiscal year 1998 audit procedures identified certain new general control vulnerabilities. Specifically, these vulnerabilities related to access controls at one of the FRB data centers and access controls, system software, and service continuity at another FRB data center. At a third FRB data center, we found vulnerabilities in access controls, application software development and change controls, segregation of duties, service continuity, and the entitywide security planning and management program. We also identified vulnerabilities in the authorization controls over one key application and vulnerabilities in the authorization and completeness controls over another key application maintained for FMS and BPD. Further, we identified vulnerabilities in authorization controls over a third key application maintained for FMS.

While these vulnerabilities do not pose significant risks to the FMS and BPD financial systems, they warrant FRB management's attention and action to decrease the risk of inappropriate disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations. The Board of Governors of the Federal Reserve System informed us that it agreed with our findings and that it had corrected or was in the process of correcting the vulnerabilities that we identified.

Background

The 12 FRBs perform fiscal agent and depository services on behalf of the U.S. government, including FMS and BPD. These services primarily consist of handling collections, such as accepting deposits of federal taxes, fees, and other receipts; providing payment-related services, such as maintaining Treasury's checking account and handling the government's disbursements, including clearing checks and making electronic payments; and providing debt-related services, such as issuing, servicing, and redeeming Treasury securities, and processing secondary market securities transfers. In fiscal year 1998, the U.S. government collected over $1.7 trillion in taxes, duties, and fines; disbursed over $1.6 trillion primarily for Social Security and veterans benefits payments, IRS tax refunds, federal employee salaries, and vendor billings; and issued more than $2 trillion in federal debt securities to the public.

---

[1] Federal Reserve Banks: Areas for Improvement in Computer Controls (GAO/AIMD-99-6, October 14, 1998).

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the computer controls over key financial management systems maintained and operated by the FRBs on behalf of FMS and BPD and to determine the status of the computer control vulnerabilities identified in our fiscal year 1997 audit. We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each data center and key application is subjected to a full-scope review that includes testing in all of the computer control areas defined in our Federal Information Systems Controls Audit Manual (FISCAM).[2] During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greater risk for computer control vulnerabilities. See appendix I for the scope and methodology of our fiscal year 1998 review at each of the selected data centers and for the key applications.

During the course of our work, we communicated our findings to FRB management who informed us that the FRBs had taken or planned to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

We performed our work at East Rutherford, New Jersey; Richmond, Virginia; Pittsburgh, Pennsylvania; San Francisco, California; St. Louis, Missouri; Minneapolis, Minnesota; Boston, Massachusetts; Philadelphia, Pennsylvania; and New York, New York, from September 1998 through January 1999. Our work was performed in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Board of Governors of the Federal Reserve System. Its comments are discussed in the "Agency Comments" section of this report and reprinted in appendix II.

---

[2] GAO/AIMD-12.19.6, January 1999.

Areas for Improvement in FRBs' General Computer Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security planning and management program, access controls, application development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security planning and management program is in place, (2) protect data, files, and programs from unauthorized access, modification, and destruction, (3) limit and monitor access to programs and files that control computer hardware and secure applications, (4) prevent the introduction of unauthorized changes to systems and applications software, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

We identified vulnerabilities in access controls, system software, application software development and change controls, segregation of duties, service continuity, and the entitywide security planning and management program. These vulnerabilities, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive data and programs, misuse or damage of computer resources, or disruption of critical operations.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and security software programs to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computing resources.

We found internal network access control vulnerabilities that increase the risk that malicious internal users with technical knowledge could potentially gain unauthorized access to computing resources and inappropriately disclose or modify sensitive data and programs or disrupt operations. However, we were not able to gain access to the production environment where the FMS and BPD applications operate. Due to the sensitive nature of the internal network control vulnerabilities we identified, these issues are described in the separate “Limited Official Use” report issued to you on August 13, 1999.

Physical security controls include locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

We found that established policies and procedures for requesting and granting physical access to an FRB data center, completing dial-in access request forms for two FRB data centers’ mainframe computers, and providing dial-in devices at one of these two data centers were not consistently enforced. We also found that informal access control procedures at one of these two FRB data centers were not always followed and were not always adequate to ensure proper accountability over and limit access to back-up tapes. At a third FRB data center, we found that procedures for authorizing and requesting access to the local area network (LAN), including maintaining the related documentation, were not consistently standardized, documented, or enforced. Failure to enforce existing access control procedures or to establish adequate formal procedures, increases the risk that individuals who were not granted explicit access privileges to computing resources could gain unauthorized or inappropriate access and potentially disrupt operations or disclose sensitive information.

System Software

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

We found, as we reported in the prior year, that the system software library at one of the FRB data centers contains library members that were no longer needed or used. Inadvertent use of obsolete or unused library members could cause unexpected operating results.

Application Software Development and Change Controls

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced.

Our review of the application software development and change control procedures at an FRB data center found that (1) change control documentation was not always developed and maintained, (2) current copies of application code are not properly archived, and (3) a separate “staging” environment for user testing prior to migrating application software changes to production is not used and an independent review and approval of changes is not required. Consequently, the risk of the unauthorized introduction and execution of program modifications is increased.

Segregation of Duties

Another key control for safeguarding programs and data is to ensure that duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as initiating, modifying, migrating, and testing of programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be appropriately segregated include applications and system programming and responsibilities for computer operations, security, and quality assurance. Policies outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced.

At one of the FRB data centers, we found that the computer operations second shift had no direct supervisor and the related activities were not routinely monitored. Consequently, inappropriate actions by the second shift operators at this data center could occur and not be detected.

Service Continuity

An organization’s ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

Because it is not cost-effective to provide the same level of continuity for all operations, it is important that organizations analyze relevant data and operations to determine which are the most critical and what resources are needed to recover and support them. As discussed in our best practices guide,[3] the criticality and sensitivity of various data and operations should be determined and prioritized based on an overall risk assessment of the entity's operations. Factors to be considered include the importance and sensitivity of the data and other organizational assets handled or protected by the individual operations and the cost of not restoring data or operations promptly.

In reviewing the FRBs' service continuity procedures, we found that one of the FRB data centers visited had updated its emergency procedures but the updated procedures had not been fully implemented. Testing of the emergency drill procedures at this data center had not been conducted in over 2 years and only a few individuals have been trained on the updated procedures. In addition, information regarding the resolution of problems identified during this data center's business resumption testing was not properly documented. At another FRB data center, we found that our prior year recommendations relating to service continuity had also not been fully implemented. We found that tests of the disaster recovery plans for one key financial application had still not been performed during the year and that compatible backup equipment had not been obtained. In addition, we found that a formal agreement between this FRB data center and its disaster recovery site for one of the key applications had not been executed. Consequently, these two data centers are at risk that, in the event of an emergency, data center personnel may not be prepared to effectively prioritize recovery activities, integrate recovery steps in an effective manner, or fully recover systems.

---

[3] Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Entitywide Security Planning and Management Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and should establish a framework for continual (1) risk assessments and development and implementation of effective security procedures and (2) monitoring and evaluation of the effectiveness of security procedures. A well-designed entitywide security planning and management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity, and that responsibilities for security are clearly understood.

Our review of one of the FRB data center's entitywide security planning and management program found that documentation evidencing the return of property, such as building access cards from terminated employees, and documentation of employee background investigations is not always retained as required by this data center's procedures. We also found that reviews of computer operations logs and violation reports were not performed routinely. Our study of information security management practices at leading nonfederal organizations found that a critical element of an effective entitywide security planning and management program is the periodic monitoring and evaluation of policy and control effectiveness to ensure controls are accomplishing their intended purposes. Noncompliance with policies and procedures increases the risk that unauthorized individuals could gain access to system resources and that such access could go undetected.

FRBs' Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs, which are used to perform a certain type of work such as generating interest payments or recording transactions in a general ledger. In an effective general control environment, application controls help to further ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

We identified vulnerabilities in the authorization controls over two key applications and vulnerabilities in the authorization and completeness controls over another key application processed for FMS and BPD.

Authorization Controls

Like general access controls, authorization controls for specific applications should be established to (1) ensure individual accountability and proper segregation of duties, (2) ensure only authorized transactions are entered into the application and processed by the computer, (3) limit the processing privileges of individuals, and (4) prevent and detect inappropriate or unauthorized activities.

We found that the existing procedures for monitoring access violation reports and related follow-up were not consistently performed for two of the key applications tested. We also found that certain customer service personnel for a third key application tested had excessive access to functions for creating or modifying information that was no longer required to perform their job responsibilities. Failure to comply with such procedures or properly limit access to sensitive application functions exposes the entity to the risk that unauthorized access to sensitive data and programs could occur and not be detected.

Completeness Controls

Completeness controls are designed to ensure that all transactions are processed and missing transactions are identified. Common completeness controls include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

During our review of controls over application data, we found that the report-writing program backup files for one of the key applications are not stored at a secure off-site location and backup policies are not written, increasing the risk that backup files may not be available to produce required reports when needed.

Conclusion

Well-designed and properly implemented general and application controls are essential to protect the FMS and BPD computer resources maintained and operated by the FRBs from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. FRB management has resolved most of the prior year vulnerabilities and has already taken some actions to resolve the new vulnerabilities we identified for fiscal year 1998. However, FRB management needs to take additional preventive measures to fully address the vulnerabilities discussed in this report and further reduce the FRBs' exposure to certain threats to its computer resources and operating environment from unintentional errors or omissions, or intentional modification, disclosure, or destruction of data and programs.

Recommendation

In our August 13, 1999, “Limited Official Use” version of this report we recommended that you (1) assign cognizant FRB officials responsibility and accountability for taking specific actions to correct each of the individual vulnerabilities that were identified during our testing and summarized in that report and (2) direct the Director of the Division of Reserve Bank Operations and Payment Systems to monitor the status of all vulnerabilities, including actions taken to correct them.

Agency Comments

In commenting on a draft of this report, the Board of Governors of the Federal Reserve System stated that overall it found the review helpful and that the information in the report will assist the Federal Reserve System in its ongoing efforts to enhance the integrity of its automated systems and information security practices. The board agreed with our assessment that FRBs have implemented effective computer controls and that while the vulnerabilities identified do not pose significant risks to the Treasury’s financial systems, they warrant FRB management’s attention. The board stated that it has corrected or will correct the vulnerabilities identified and will implement the report recommendation to assign the appropriate Reserve Bank officials responsibility for correcting the individual vulnerabilities in the report. We will follow up on these matters during our audit of the federal government’s fiscal year 1999 financial statements.

We are sending copies of this report to Senator Robert C. Byrd, Senator Ben Nighthorse Campbell, Senator Pete V. Domenici, Senator Byron L. Dorgan, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, Senator Fred Thompson, and to Representative Bill Archer, Representative Dan Burton, Representative Stephen Horn, Representative Steny H. Hoyer, Representative John R. Kasich, Representative Jim Kolbe, Representative David R. Obey, Representative Charles B. Rangel, Representative John M. Spratt, Representative Jim Turner, Jr., Representative C.W. Bill Young, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcommittees. We are also sending copies of this report to the

Honorable Jacob Lew, Director of the Office of Management and Budget and certain FRB officials. We will send copies to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were Christine A. Robertson, J. Lawrence Malenich, Paula M. Rascona, and Gregory C. Wilshusen.

Sincerely yours,

Gary T. Engel

Gary T. Engel
Associate Director
Governmentwide Accounting and
Financial Management Issues

Contents

Letter 1

Appendix I Scope and Methodology 14

Appendix II Comments From the Board of Governors of the Federal Reserve System 17

Abbreviations

BPD	Bureau of the Public Debt
FISCAM	Federal Information Systems Controls Audit Manual
FMS	Financial Management Service
FRB	Federal Reserve Bank
ID	identification
LAN	local area network

Appendix I

Scope and Methodology

We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each data center and key application is subjected to a full-scope review that includes testing in all of the computer control areas defined in the FISCAM. During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greater risk for computer control vulnerabilities.

The scope of our work for fiscal year 1998 included follow-up on vulnerabilities identified in our fiscal year 1997 audit and

- a focused review at one of the FRB data centers of the three general controls areas intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction;
  - limit and monitor access to programs and files that control computer hardware and secure applications; and
  - prevent the introduction of unauthorized changes to systems and applications software;
- a focused review at another of the FRB data centers of the three general controls areas intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction;
  - limit and monitor access to programs and files that control computer hardware and secure applications; and
  - ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- a full-scope review at a third FRB data center of the general controls intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction;
  - limit and monitor access to programs and files that control computer hardware and secure applications;
  - prevent the introduction of unauthorized changes to systems and applications software;
  - prevent any one individual from controlling key aspects of computer-related operations;
  - ensure that an adequate computer security planning and management program is in place; and
  - ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

To evaluate these general controls, we identified and reviewed the FRBs' information system general control policies and procedures, conducted tests and observed controls in operation, and held discussions with officials at selected FRB data centers to determine whether controls were in place, adequately designed, and operating effectively. Our penetration testing was expanded this year to also include internal penetration testing procedures. Through our internal and external penetration testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of certain FRB officials.

We performed a full-scope application controls review of three key applications to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely;
- data are properly processed by the computer and files are updated correctly;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

The scope of our work over another three key applications included follow-up on vulnerabilities that we identified in our fiscal year 1997 audit and focused on the following three application control areas to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely; and
- data are properly processed by the computer and files are updated correctly.

The scope of our work over a seventh key application included follow-up on vulnerabilities that we identified in our fiscal year 1997 audit and focused on the following two application control areas to determine whether the application is designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities and
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely.

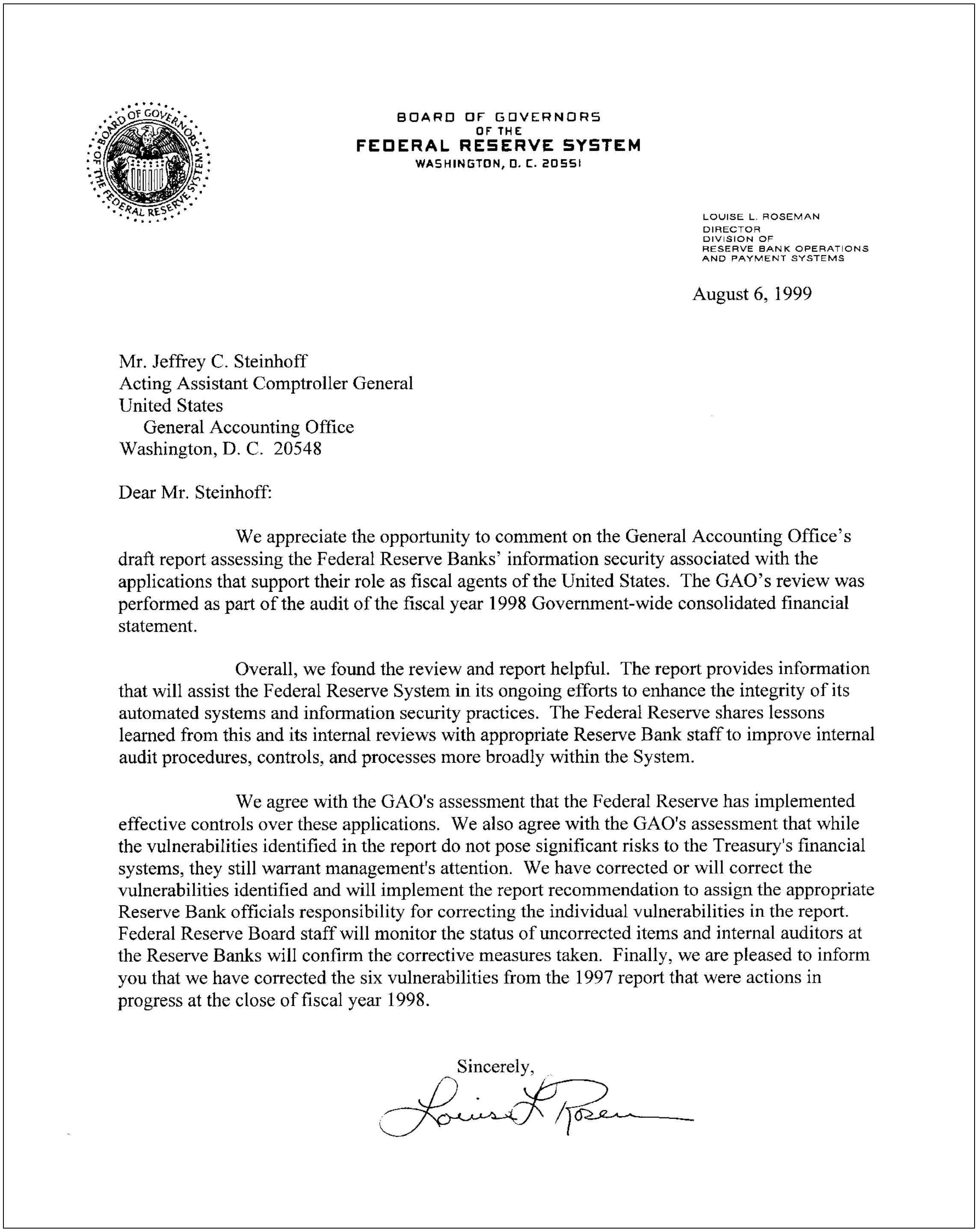
We also reviewed the application computer controls audit work performed by the FRB internal auditors over two key applications.

To assist in our evaluation and testing of computer controls, we contracted with the independent public accounting firm PricewaterhouseCoopers LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related workpapers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated our findings to FRB management who informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

We performed our work at East Rutherford, New Jersey; Richmond, Virginia; Pittsburgh, Pennsylvania; San Francisco, California; St. Louis, Missouri; Minneapolis, Minnesota; Boston, Massachusetts; Philadelphia, Pennsylvania; and New York, New York, from September 1998 through January 1999. Our work was performed in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Board of Governors of the Federal Reserve System. Its comments are discussed in the "Agency Comments" section of this report and are reprinted in appendix II.

Comments From the Board of Governors of the Federal Reserve System



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

LOUISE L. ROSEMAN
DIRECTOR
DIVISION OF
RESERVE BANK OPERATIONS
AND PAYMENT SYSTEMS

August 6, 1999

Mr. Jeffrey C. Steinhoff
Acting Assistant Comptroller General
United States
General Accounting Office
Washington, D. C. 20548

Dear Mr. Steinhoff:

We appreciate the opportunity to comment on the General Accounting Office's draft report assessing the Federal Reserve Banks' information security associated with the applications that support their role as fiscal agents of the United States. The GAO's review was performed as part of the audit of the fiscal year 1998 Government-wide consolidated financial statement.

Overall, we found the review and report helpful. The report provides information that will assist the Federal Reserve System in its ongoing efforts to enhance the integrity of its automated systems and information security practices. The Federal Reserve shares lessons learned from this and its internal reviews with appropriate Reserve Bank staff to improve internal audit procedures, controls, and processes more broadly within the System.

We agree with the GAO's assessment that the Federal Reserve has implemented effective controls over these applications. We also agree with the GAO's assessment that while the vulnerabilities identified in the report do not pose significant risks to the Treasury's financial systems, they still warrant management's attention. We have corrected or will correct the vulnerabilities identified and will implement the report recommendation to assign the appropriate Reserve Bank officials responsibility for correcting the individual vulnerabilities in the report. Federal Reserve Board staff will monitor the status of uncorrected items and internal auditors at the Reserve Banks will confirm the corrective measures taken. Finally, we are pleased to inform you that we have corrected the six vulnerabilities from the 1997 report that were actions in progress at the close of fiscal year 1998.

Sincerely,

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00

[redacted]