United States General Accounting Office

GAO

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

October 1998

FEDERAL RESERVE BANKS

Areas for Improvement in Computer Controls

GAO/AIMD-99-6

GAO

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

Accounting and Information
Management Division

B-280753

October 14, 1998

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

Dear Mr. Chairman:

We recently reported on the U.S. government's consolidated financial statements for fiscal year 1997 (GAO/AIMD-98-127, March 31, 1998). Our audit was done pursuant to the Chief Financial Officers Act of 1990, as expanded by the Government Management Reform Act of 1994. Our review of the general and application computer controls over key Financial Management Service (FMS) and Bureau of the Public Debt (BPD) financial systems maintained and operated by the 12 Federal Reserve Banks (FRB) was performed as part of this audit. Today, we issued a "Limited Official Use" report detailing vulnerabilities in both general and application computer controls. This version of the excerpted report for public release provides a general summary of the vulnerabilities we identified and the recommendation we made.

This report discusses general and application controls over the key FMS and BPD financial systems that are maintained and operated by FRBs. FRBs, as fiscal agents and depositories of the federal government, provide services that primarily consist of handling collections, disbursements, and issuance and redemption of debt.

General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They are intended to (1) protect data, files, and programs from unauthorized access, modification, and destruction, (2) prevent the introduction of unauthorized changes to systems and applications software, (3) ensure that system software development and maintenance, applications software development and maintenance, computer operations, security, and quality assurance functions are performed by different people, (4) ensure recovery of computer processing operations in case of a disaster or other unexpected interruption, and (5) ensure that an adequate computer security planning and management program is in place.

Application controls are the structure, policies, and procedures that apply to individual application systems. These controls help to ensure that

transactions are valid, properly authorized, and completely and accurately processed by the computer.

We found that FRBs had implemented effective computer controls over key BPD and FMS financial systems that they maintained and operated. However, as discussed in this report, we identified vulnerabilities involving computer controls that if left uncorrected, could increase the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations. These vulnerabilities warrant FRB management's attention and action.

During the process of performing our work, we provided detailed information on our interim findings and recommended corrective actions to FRB management. This report summarizes those findings.

Results in Brief

Overall, we found that FRBs had implemented effective computer controls. However, we identified vulnerabilities in computer controls involving (1) access to systems, programs, and data, including unauthorized external access, (2) service continuity and contingency planning, and (3) access controls over certain financial applications. While these vulnerabilities do not pose significant risks to the BPD and FMS financial systems, they warrant FRB management's attention and action to decrease the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations.

FRBs have corrected or are correcting the vulnerabilities that we identified. The following discussion provides a general summary of the vulnerabilities that existed on September 30, 1997. Those that we verified had been fully resolved subsequent to September 30, 1997, we have so noted. We will review the status of FRBs' corrective actions during our audit of the federal government's fiscal year 1998 consolidated financial statements.

Background

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, processing secondary market transactions,

and handling the related transfers of funds. In fiscal year 1997, Treasury collected over $1.5 trillion in taxes, duties, and fines; disbursed approximately $1 trillion for Social Security and Veterans benefits, tax refunds, federal employee salaries, and vendor billings; and issued more than $2 trillion in public debt.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the general computer and application controls over key financial management systems maintained and operated by FRBs on behalf of FMS and BPD.

Specifically, we evaluated general controls intended to

- protect data, files, and programs from unauthorized access, modification, and destruction;
- prevent the introduction of unauthorized changes to systems and applications software;
- provide adequate segregation of duties involving applications and system programmers and of responsibilities for computer operations, security, and quality assurance;
- ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an adequate computer security planning and management program is in place.

To evaluate general controls, we identified and reviewed FRBs' information system general control policies and procedures, conducted tests and observations of controls in operation, and held discussions with officials at the locations visited to determine whether the FRB general controls were in place, adequately designed, and operating effectively. Further, we attempted to obtain access to sensitive data and programs. These attempts, referred to as penetration testing, were performed with the knowledge and cooperation of FRB officials.

We also evaluated application controls intended to ensure that

- access privileges establish individual accountability and proper segregation of duties, limit the processing privileges of individuals, and 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; 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.

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

During the course of our work, we communicated interim findings and recommended corrective actions to FRB management who informed us that FRBs have taken or plan to take corrective action to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the federal government's fiscal year 1998 consolidated financial statements.

We performed our work at FRB data centers in Atlanta, Georgia; Minneapolis, Minnesota; New York, New York; Pittsburgh, Pennsylvania; Richmond, Virginia; East Rutherford, New Jersey; San Francisco, California; and Dallas, Texas, from March 1997 through January 1998 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Chairman of the Board of Governors of the Federal Reserve System or his designee. The board's comments are reprinted in appendix I.

Areas for Improvement in General Computer Controls

Our review of the FRB general computer controls did not identify any weaknesses that placed the financial systems operated and maintained for FMS and BPD at significant risk of being accessed, compromised, or destroyed. However, we identified vulnerabilities in access controls and service continuity and contingency planning that warrant management's attention and action. These vulnerabilities, if left uncorrected, increase the risk that inappropriate disclosure or modification of sensitive information or disruption of critical operations could occur and not be detected or prevented in a timely manner.

Access Controls

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

Logical controls include user identifications (ID), passwords, or other identifiers and security software programs. Logical controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and to prevent unauthorized users from gaining access to computing resources. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

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 espionage, sabotage, damage, and theft.

Our review of FRB access controls identified vulnerabilities that related to (1) granting systems privileges to users, (2) management of passwords and user IDs, (3) setting security software options in a manner to ensure optimum security or appropriate segregation of duties, (4) management of physical access to certain system resources, and (5) management of local area network and Internet dial-in activities.

We verified that corrective actions to resolve two of the individual vulnerabilities had been completed by FRBs subsequent to September 30, 1997.

Service Continuity and Contingency Planning

An organization's ability to accomplish its mission can be significantly impacted 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) contingency plans for recovering critical operations should interruptions occur.

A contingency 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 prioritizes resources in order of criticality. To be most effective, a contingency plan should be periodically tested and employees should be trained in and familiar with its use.

In reviewing FRBs' service continuity and contingency planning, we found that adequate tests of certain aspects of the disaster recovery plans were not being conducted at two sites and plans and related backup equipment for one financial system were not updated to accommodate system changes.

Application Controls Can Be Strengthened

Our review of the FRB application controls over financial systems operated and maintained for FMS and BPD identified opportunities for improvements in authorization controls.

Authorization Controls

Authorization controls are designed to ensure that only approved transactions are entered into the application systems and processed by the computer. We found problems related to (1) limiting users to those system processing functions and transactions required for the users' job responsibilities and (2) inadequate or incomplete documentation for granting users access to applications.

Conclusion

Overall, we found that FRBs had implemented effective computer controls over key BPD and FMS financial systems that they maintained and operated. However, we identified vulnerabilities that, while they do not pose significant risks to the BPD and FMS financial systems, warrant FRB management's attention and action to decrease the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations.

Recommendation

To improve areas of vulnerability in general controls and application controls cited in our "Limited Official Use" version of this report, we recommended that you (1) assign cognizant FRB officials responsibility and accountability for correcting each individual vulnerability that we identified and communicated to FRB management during our testing 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.

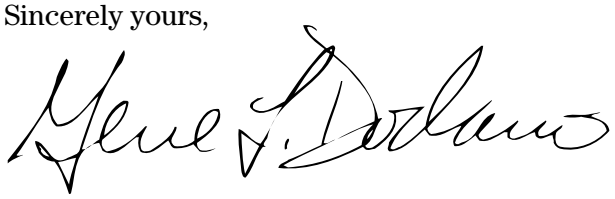
Agency Comments

In commenting on a draft of this report, the Board of Governors of the Federal Reserve System 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 they have implemented our recommendation and that FRBs are in the process of correcting the vulnerabilities identified in our report to the extent possible. We will follow up on these matters during our audit of the federal government's fiscal year 1998 consolidated financial statements. In addition to its written comments, the staff of the Board of Governors of the Federal Reserve System provided technical comments, which have been incorporated as appropriate.

We are sending copies of this report to the Director of the Office of Management and Budget, and to the Chairmen and Ranking Minority Members of the Senate Committee on Appropriations and its Subcommittee on Treasury and General Government; Senate Committee on Finance; Senate Committee on Governmental Affairs; Senate Committee on the Budget; House Committee on Appropriations and its Subcommittee on Treasury, Postal Service, and General Government; House Committee on Ways and Means; House Committee on Government Reform and Oversight and its Subcommittee on Government Management, Information and Technology; and House Committee on the Budget. We will also send copies to others upon request.

This work was performed under the direction of Gary T. Engel, Associate Director, Governmentwide Audit and Financial Management Issues, who can be reached at (202) 512-3406. Other major contributors to this report are listed in appendix II.

Sincerely yours,



Gene L. Dodaro
Assistant Comptroller General

Contents

Abbreviations

BPD	Bureau of the Public Debt
FMS	Financial Management Service
FRB	Federal Reserve Bank
ID	identification

Comments From the Federal Reserve System

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

CLYDE H. FARNSWORTH, JR.
DIRECTOR
DIVISION OF
RESERVE BANK OPERATIONS
AND PAYMENT SYSTEMS

September 4, 1998

Mr. Gene L. Dodaro
Assistant Comptroller General
United States General
Accounting Office
Washington, D. C. 20548

Dear Mr. Dodaro:

We appreciate the opportunity to respond to 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 1997 Governmentwide consolidated financial statement.

We agree with the GAO's assessment that the Federal Reserve has implemented effective computer controls over these applications. We also agree with the GAO's statement that while the vulnerabilities identified in the report do not pose significant risks to the Treasury's financial systems, they warrant management's attention. We have corrected or will correct the vulnerabilities to the extent possible and have implemented the report recommendation. Federal Reserve Board staff has provided general oversight of this process and the independent, internal auditors at the Reserve Banks will confirm the corrective measures taken.

Sincerely,

Clyde H. Farnsworth, Jr.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Christine A. Robertson, Assistant Director
Paula M. Rascona, Audit Manager
Gregory C. Wilshusen, Assistant Director - Technical Advisor

Ordering Information

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested