

July 2000

FEDERAL RESERVE BANKS

Areas for Improvement in Computer Controls



G A O

Accountability * Integrity * Reliability



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

**Accounting and Information
Management Division**

B-285042

July 7, 2000

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

Dear Mr. Greenspan:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1999 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 the Bureau of the Public Debt (BPD).¹ On May 18, 2000, 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 presents the results of our fiscal year 1999 tests of the effectiveness of general and application controls that support key FMS and BPD automated financial systems maintained and operated by the FRBs and our follow-up on the status of the FRBs' corrective actions to address vulnerabilities identified in our audits for fiscal years 1998 and 1997.

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 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 and the recommendation we made.

¹31 U.S.C. 331(e) (1994).

Results in Brief

While we found that the FRBs had implemented effective general and application controls, our fiscal year 1999 audit procedures identified certain general and application control vulnerabilities. These vulnerabilities relate to the entitywide security management program at a data center; the entitywide security management program, access controls, and system software at a second data center; access controls at one FRB; entitywide security management program and access controls at a third data center; and access controls, system software, application software development and change controls, and segregation of duties at a fourth data center. We also identified vulnerabilities relating to authorization controls over two key applications.

Our follow-up on the status of the FRBs' corrective actions to address vulnerabilities identified in our audits for fiscal years 1998 and 1997 found that the FRBs had corrected or mitigated the risks associated with 19 of the 30 general and application control vulnerabilities discussed in our prior reports.²

While these vulnerabilities do not pose significant risks to the FMS and BPD financial systems, they warrant FRB management's action to decrease the risk of inappropriate disclosure and modification of sensitive data and programs, misuse of or damage to computer resources, or disruption of critical operations. In commenting on a draft of this report and our more detailed Limited Official Use report, the Board of Governors of the FRB informed us that it agreed with 17 of our 22 findings and had corrected or was in the process of correcting those findings. Further, the board stated that it is studying the remaining five findings before developing and implementing corrective actions.

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 collection handling functions, 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

²*Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO-AIMD-99-280, Sept. 15, 1999).

redeeming Treasury securities and processing secondary market securities transfers. In fiscal year 1999, the U.S. government collected over \$1.8 trillion in taxes, duties, and fines; disbursed over \$1.7 trillion primarily for Social Security and veterans benefits payments, IRS tax refunds, federal employee salaries, and vendor billings; and issued about \$2.2 trillion in federal debt securities to the public.

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 actions taken to address the computer control vulnerabilities identified in our audits for fiscal years 1998 and 1997. We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each significant 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 System Controls Audit Manual (FISCAM).³ 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 1999 review at each of the selected data centers and for the selected key applications.

During the course of our work, we communicated our findings to FRB management which 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 2000 financial statements.

We performed our work at East Rutherford, New Jersey; Richmond, Virginia; Pittsburgh, Pennsylvania; Dallas, Texas; St. Louis, Missouri; Minneapolis, Minnesota; Atlanta, Georgia; and New York, New York, from July 1999 through January 2000. 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.

³*Federal Information System Controls Audit Manual, Volume I – Financial Statement Audits* (GAO/AIMD-12.19.6, Jan. 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 management program, access controls, system software, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would help (1) ensure that an adequate entitywide program for security management is in place, (2) protect data, files, and programs from unauthorized access, modification, disclosure, 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.

Entitywide Security Management Program

We identified vulnerabilities in the entitywide security management program, access controls, system software, application software development and change controls, and segregation of duties. 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.

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 assessment and development and implementation of effective security procedures and (2) monitoring and evaluation of the effectiveness of security procedures. A well-designed entitywide security 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 FRB data center's entitywide security management program noted that at the time of our review, periodic reinvestigations of data center personnel holding sensitive positions were not being conducted nor were they required. As a result, there is an increased risk at this data center that management will not be made aware of changes to an employee's personal situation that would cause the employee to be ineligible to hold a sensitive position.

At two other FRB data centers, we found that sections of the operations manuals were outdated and that policies did not require periodic review to ensure that the manuals remained current. As a result, computer operations are vulnerable to staff not correctly performing their duties. At one of these two data centers, we also found that all officers were required to take one leave period of at least 5 days annually, but there was no similar requirement for other data center employees. Further, remote access capabilities are not suspended while an employee is on vacation, and there is no formal policy requiring the periodic review and recertification of users' remote access capabilities. Unauthorized activities are less likely to be discovered when employees take fewer than 5 days of vacation and when remote access capabilities are not suspended while an employee is on vacation.

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 they prevent unauthorized users from gaining access to computing resources.

In connection with our testing at one data center, we found internal network access control vulnerabilities at one FRB. At another data center, we found inappropriate access to system resources. These vulnerabilities increased the risk that malicious internal users with technical knowledge could gain unauthorized access to computing resources and inappropriately disclose or modify data or programs. However, we were not able to gain unauthorized access to the production environment where the FMS and BPD applications operate. Because of 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 May 18, 2000.

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 loss or impairment by limiting access to the buildings and rooms where they are housed. We found inconsistent practices for providing access to sensitive and secure areas at one data center. These practices increase the risk of unauthorized access to sensitive areas of the data center.

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 integrity and reliability of information systems.

At one FRB data center, we found that system software Authorized Program Facilities (APF) libraries were not always at their designated locations or that members listed in the APF libraries were obsolete. Also, there were several programs in different APF libraries that could potentially be different versions of the same programs. This increased the risk that an incorrect version of the program or an unauthorized program could execute and cause unexpected operating results.

At another FRB data center, we found that basic system software policies and procedures do not include sufficient detail to ensure that management-approved practices to implement releases of system software will be followed.

We also found at this same data center that certain vulnerabilities reported in the prior year continue. These vulnerabilities potentially could give multiple users the opportunity to exploit or gain access to computer resources. In addition, we found that a variety of application tools were not being used or not being used as effectively as possible. These vulnerabilities increased the risk of unauthorized access to sensitive files or disruption of operations.

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 one FRB data center found that (1) the change control process was not always consistently documented, (2) a formal process had not been established for informing personnel responsible for the software archives about changes to the source code libraries, and (3) a separate environment had not been established to protect tested and user-approved changes from unauthorized modification before moving them into production. As a result, 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 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 FRB data center, as we reported in the prior year, we found that the computer operations second shift continued to have no direct supervisor and there was no evidence that related activities were routinely monitored. Consequently, inappropriate actions by the second shift operators could occur and not be detected.

FRBs' Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs, each of which is 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.

Authorization Controls

Authorization controls for specific applications, like general access controls, should be established to help (1) ensure individual accountability

and proper segregation of duties, (2) ensure that 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 for two key applications, the procedures for monitoring access violation memos and related follow-up were sometimes not clearly defined. Noncompliance with procedures exposes the entity to the risk that unauthorized access to sensitive data and programs could occur and not be detected promptly.

We also found for one of these applications that several retired group user IDs continue to exist and if activated could give inappropriate access to implement unauthorized system changes without detection.

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 risk of inappropriate disclosure and modification of sensitive information, misuse of or damage to computer resources, and disruption of critical operations. FRB management has resolved many of the prior years' vulnerabilities and has already taken some actions to resolve the new vulnerabilities we identified for fiscal year 1999. However, FRB management needs to take additional preventive measures to fully address the vulnerabilities discussed in this report and to further reduce the FRBs' exposure to threats to their computer resources and operating environment from errors, unintentional omissions, or intentional modification, disclosure, or destruction of data and programs.

Recommendation

In our May 18, 2000, Limited Official Use version of this report, we recommended that you (1) assign to cognizant FRB officials responsibility and accountability for correcting each vulnerability that we 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

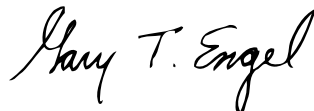
In commenting on a draft of this report, the Board of Governors of the Federal Reserve System stated that overall it found the review helpful and

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 Treasury's financial systems, they warrant FRB management's attention. The board stated that it has corrected or will correct most of the vulnerabilities identified in this report and will study the others before developing and implementing corrective actions. We will follow up on these matters during our audit of the federal government's fiscal year 2000 financial statements.

We are sending copies of this report to Senator Robert C. Byrd, Senator Pete V. Domenici, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, Senator Fred Thompson, Representative Bill Archer, Representative Spencer Bachus, Representative Dan Burton, Representative Stephen Horn, Representative John R. Kasich, Representative David R. Obey, Representative Charles B. Rangel, Representative John M. Spratt, Jr., Representative Jim Turner, Jr., Representative Maxine Waters, Representative Henry A. Waxman, and Representative C. W. Bill Young 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 J. Lew, Director of the Office of Management and Budget, and the Honorable Jeffery Rush, Jr., Inspector General, Department of the Treasury.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were Paula M. Rascona and Daniel G. Mesler.

Sincerely yours,



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

Scope and Methodology

We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each significant 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 1999 included follow-up on vulnerabilities identified in our audits for fiscal years 1998 and 1997 and a focused review

- at the first data center, of the two general control areas intended to
 - ensure that an adequate entitywide computer security management program is in place and
 - prevent any one individual from controlling key aspects of computer-related operations;
- at the second data center, of the three general control areas intended to
 - protect data, files, and programs from unauthorized access, modification, disclosure, and destruction;
 - limit and monitor access to programs and files that control computer hardware and secure applications; and
 - prevent any one individual from controlling key aspects of computer-related operations;
- at the third data center, of the two general control areas intended to
 - protect data, files, and programs from unauthorized access, modification, disclosure, and destruction and
 - prevent any one individual from controlling key aspects of computer-related operations; and
- at the fourth data center, of the general control area intended to
 - ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

We limited our work at two other data centers to a follow-up review of the status of actions taken to address the vulnerabilities identified in our fiscal year 1997 audit.

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. 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 promptly;
- 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 key application 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 promptly.

We limited our work on two additional key applications to a follow-up review of the status of actions taken to address the vulnerabilities identified in our fiscal year 1998 audit.

We also reviewed the application computer controls audit work performed by the FRB internal auditors on two more 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 findings were adequately supported.

During the course of our work, we communicated our findings to FRB management which has 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 2000 financial statements.

We performed our work at East Rutherford, New Jersey; Richmond, Virginia; Pittsburgh, Pennsylvania; Dallas, Texas; St. Louis, Missouri; Minneapolis, Minnesota; Atlanta, Georgia; and New York, New York, from July 1999 through January 2000. 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.

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

April 27, 2000

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 U.S. government's fiscal year 1999 financial statements.

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 17 of the 22 vulnerabilities identified in the report, but the remaining five will require further study before corrective actions can be developed and fully implemented. Federal Reserve Board staff will monitor the status of uncorrected items and items under study. Internal auditors at the Reserve Banks will confirm the corrective measures taken.

Sincerely,

A handwritten signature in cursive script, reading "Louise L. Roseman".

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. 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

Orders by visiting:

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

Orders by phone:

(202) 512-6000
fax: (202) 512-6061
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.

Orders by Internet:

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>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

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

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Rate Postage & Fees Paid GAO Permit No. GI00</p>

