GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

December 10, 2001

Louise L. Roseman, Director
Division of Reserve Bank Operations
and Payment Systems
Board of Governors of the Federal
Reserve System

Subject: Federal Reserve Banks: Areas for Improvement in Computer Controls

Dear Ms. Roseman:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 2000 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 August 30, 2001, we issued a Limited Official Use letter to you detailing the results of our review. This excerpted version of the letter for public release summarizes the vulnerabilities we identified and the recommendation we made.

This letter presents the results of our fiscal year 2000 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 audit for fiscal year 1999.

Overall, we found that the FRBs had implemented effective general and application controls. However, as discussed in this letter, 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 that nonetheless warrant FRB management's action. In addition to the Limited Official Use letter provided to management, we communicated detailed information regarding our findings to appropriate FRB managers during our audit.

Results in Brief

Our fiscal year 2000 audit procedures identified opportunities to improve general controls related to access at two data centers; access, system software, and service

[1] 31 U.S.C. 331(e) (1994).

continuity at a third data center; and access and system software at a fourth data center. We also identified opportunities to improve authorization controls over four key applications and accuracy controls over one of these key applications.

Our follow-up on the status of the FRBs' corrective actions to address vulnerabilities identified in our prior years' audits found that the FRBs had corrected or mitigated the risks associated with all the general and application control vulnerabilities discussed in our prior report.[2] Overall, we found that the FRBs had implemented effective general and application controls.

While the general and application control vulnerabilities we identified do not pose significant risks to the FMS and BPD financial systems, they warrant the FRB manager's action to decrease the risk of inappropriate disclosure and modification of sensitive data and programs, misuse of or damage to computer resources, and disruption of critical operations. In commenting on a draft of this letter and our more detailed Limited Official Use letter, 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 most of the vulnerabilities we identified and will conduct further discussions with us on the remaining ones.

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 redeeming Treasury securities and processing secondary market securities transfers. In fiscal year 2000, the U.S. government collected over $2 trillion in taxes, duties, and fines; disbursed over $1.9 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. The FRB data centers maintain and operate an array of financial and information systems to process and reconcile monies disbursed and collected on behalf of FMS and BPD.

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 1999, 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

[2] *Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO/AIMD-00-218, July 7, 2000).
[3] *Federal Information System Controls Audit Manual, Volume I – Financial Statement Audits* (GAO/AIMD-12.19.6, Jan. 1999).

the FISCAM areas that we have determined are at greater risk for computer control vulnerabilities. See enclosure I for a more detailed discussion of the scope and methodology of our fiscal year 2000 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 managers who informed us that the FRBs had corrected or planned to correct the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2001 financial statements.

We performed our work at select FRB data centers from July 2000 through January 2001. Our work was performed in accordance with U.S. generally accepted government auditing standards. We requested comments on a draft of this letter from the Board of Governors of the Federal Reserve System. Its comments are discussed in the "Agency Comments" section of this letter and reprinted in enclosure II.

Opportunities for Strengthening 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 helps (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.

We identified opportunities to improve the FRB's access controls, system software, and service continuity. The vulnerabilities we identified, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive data and programs, misuse or damage of computer resources, and 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 physical and logical security controls.

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. To improve physical security controls at one data center, appropriate documentation needs to be maintained to help ensure that appropriate access rights are granted and that policies related to accessing sensitive areas are

understood. Physical security controls at two other data centers can be improved in the areas of key-card issuance and documentation using an access-request form.

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. At two data centers, improvements are needed in controls over passwords. In addition, at one of these data centers, appropriate controls over access to system resources need to be established to (1) limit users to those system files and resources needed to perform their jobs, (2) ensure user access is approved, and (3) limit the establishment of groups of access privileges to those needed and used.

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. To help ensure that an incorrect version of a program or an unauthorized program could not execute and cause unexpected results or disruption of operations, one data center needs to strengthen its procedures and processes for introducing system software changes into production. To improve system software controls at another FRB data center, steps should be taken to (1) enhance the security over information maintained in databases and job submission processes, (2) limit the ability to perform administrative activities and view or obtain system information and utilities, (3) enforce the use of strong passwords, and (4) ensure that sensitive system activities are logged and monitored.

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. One data center needs to limit the risk that changes to data

processing or recovery needs are not properly communicated when changes to the computer resources occur.

Certain FRB Application Controls Can Be Strengthened

Application controls relate directly to 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 opportunities for improvement in the authorization controls over four key applications and accuracy controls over one of these four key applications.

Authorization Controls

Authorization controls for specific applications, such as 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. For three key applications, controls need to be enhanced to help further ensure that obsolete and inactive user IDs are promptly removed. Authorization controls over two key applications can also be enhanced to ensure that access-request forms are completed entirely. For one key application, additional controls are needed to limit to users with a business need access to the application and the ability to update or modify it. Enhancing these controls will help prevent unauthorized access to the applications and sensitive information.

Accuracy Controls

The recording of valid and accurate data into application systems is essential to an effective system that produces reliable results. Accuracy controls include (1) well-designed data entry procedures, (2) data validation and editing to identify erroneous data, (3) reporting, investigating, and correcting erroneous data, and (4) review and reconciliation of output. To help ensure that data entered into one key application are accurate, modifications to the edit screen are 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 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 the prior years' vulnerabilities and has already acted to resolve the new vulnerabilities we identified for fiscal year 2000. However, management attention is needed to fully address the vulnerabilities discussed in this letter and to further reduce the FRBs' exposure to threats to their computer resources and operating environment from errors; unintentional omissions; and intentional modification, disclosure, or destruction of data and programs.

Recommendation for Executive Action

In our August 30, 2001, Limited Official Use version of this letter, we recommended that you assign to cognizant FRB officials responsibility and accountability for correcting each vulnerability that we identified and for addressing each of the specific recommendations detailed in the enclosure to that letter.

Agency Comments

In commenting on a draft of this letter, the Board of Governors of the Federal Reserve System stated that overall it found the review helpful and that the information in the letter 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 letter and will conduct further discussions with us on the remaining ones. We will follow up on these matters during our audit of the federal government's fiscal year 2001 financial statements. In addition to its written comments, the staff of the FRBs provided technical comments, which have been incorporated as appropriate.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Appropriations; Senate Committee on Finance; Senate Committee on Governmental Affairs; Senate Committee on the Budget; Subcommittee on Treasury and General Government, Senate Committee on Appropriations; House Committee on Appropriations; House Committee on Ways and Means; House Committee on Government Reform; House Committee on the Budget; Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, House Committee on Government Reform; Subcommittee on Treasury, Postal Service, and General Government, House Committee on Appropriations; and House Committee on Financial Services. We are also sending copies of this letter to the Chairman of the Board of Governors of the Federal Reserve System and the Director of the Office of Management and Budget.

If you have any questions regarding this letter, please contact Paula M. Rascona, Assistant Director, at (202) 512-9816. Other key contributors to this assignment were Louise DiBenedetto, Dean Carpenter, and Mickie Gray.

Sincerely yours,

Gary T. Engel

Gary T. Engel
Director
Financial Management and Assurance

Enclosure 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 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 FISCAM. During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greatest risk for computer control vulnerabilities.

The scope of our work for fiscal year 2000 included follow-up on vulnerabilities identified in our audit for fiscal year 1999 and a focused review at

- two FRB data centers, of the general control area intended to
    - protect data, files, and programs from unauthorized access, modification, disclosure, and destruction;
- a third FRB 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
    - ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.
- a fourth FRB data center, of the two general control areas intended to
    - protect data, files, and programs from unauthorized access, modification, disclosure, and destruction; and
    - limit and monitor access to programs and files that control computer hardware and secure applications.

We limited our work at a fifth FRB data center to a follow-up review of the status of actions taken to address the vulnerabilities identified in our fiscal years 1999, 1998, and 1997 audits.

We limited our testing of the FRB entitywide security program to a comparison of the FRB's information security manual with our *Executive Guide on Information Security Management.*[4]

To evaluate these general controls, we identified and reviewed the FRBs' information system general control policies and procedures; observed controls in operation; conducted tests of controls using a method in which the results are not projectable to the population; and held discussions with officials at selected FRB data centers to

[4]*Executive Guide: Information Security Management* (GAO/AIMD-98-68, May 1998).

determine whether controls were in place, adequately designed, and operating effectively. Through our internal and external vulnerability assessment testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of appropriate FRB officials.

We performed full-scope application control reviews of four 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.

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 years 1999 and 1998 audits.

To evaluate application controls, we identified and reviewed FRBs' information system application control policies and procedures; observed controls in operation; tested controls, using a method in which the results are not projectable to the population; and discussed with officials at the selected FRB data centers whether controls were in place, adequately designed, and operating effectively.

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 working papers to ensure that the findings were adequately supported.

During the course of our work, we communicated our findings to FRB managers who have informed us that the FRBs have corrected or plan to correct the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2001 financial statements.

We performed our work from July 2000 through January 2001. Our work was performed in accordance with U.S. generally accepted government auditing standards. We requested comments on a draft of this letter from the Board of Governors of the Federal Reserve System. Its comments are discussed in the "Agency Comments" section of this letter and reprinted in enclosure II.

Enclosure 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 22, 2001

Mr. Gary T. Engel
Director
Financial Management and Assurance
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Engel:

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 2000 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 review and its internal reviews with appropriate Federal Reserve staff to improve internal audit procedures, controls, and processes more broadly within the System.

We agree with 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. Of the 29 vulnerabilities identified in the report, we have corrected or will correct 20, four others require further study and discussion with GAO, and five are addressed by existing compensating controls. Federal Reserve Board staff will monitor the status of uncorrected items and items under study. Internal auditors at the Reserve Banks will confirm all corrective measures taken.

Sincerely,

Louise Roseman
for LR

(198060)