G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 16, 2008

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 Information Security Controls*

Dear Ms. Roseman:

In connection with fulfilling our requirement to audit the financial statements of the U.S. government,[1] we audited and reported on the Schedules of Federal Debt Managed by the Bureau of the Public Debt (BPD) for the fiscal years ended September 30, 2007 and 2006.[2] As part of these audits, we performed a review of the general and application information security controls over key financial systems maintained and operated by the Federal Reserve Banks (FRBs) on behalf of the Department of the Treasury's BPD relevant to the Schedule of Federal Debt.

In our audit report on the Schedules of Federal Debt for the fiscal years ended September 30, 2007 and 2006, we concluded that BPD maintained, in all material respects, effective internal control relevant to the Schedule of Federal Debt related to financial reporting and compliance with applicable laws and regulations as of September 30, 2007, that provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt would be prevented or detected on a timely basis. However, we found matters involving information security controls that we do not consider to be significant deficiencies.[3] As it relates to controls over financial reporting and compliance with applicable laws and regulations, the potential effect of such control deficiencies was mitigated by the

[1]31 U.S.C. § 331(e).

[2]GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2007 and 2006 Schedules of Federal Debt*, GAO-08-168 (Washington, D.C.: Nov. 7, 2007).

[3]A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions to prevent or detect misstatements on a timely basis.

FRBs and BPD. The FRBs mitigated the potential effect of such control deficiencies with physical security measures and a program of monitoring user and system activity, and BPD with compensating management and reconciliation controls. Nevertheless, the matters relating to key financial systems maintained and operated by the FRBs on behalf of BPD warrant FRB management's attention and action.

This report presents the control deficiencies identified during our fiscal year 2007 testing of the general and application information security controls over key financial systems maintained and operated by the FRBs on behalf of the Department of the Treasury's BPD relevant to the Schedule of Federal Debt. In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to FRB management.

Results in Brief

Our fiscal year 2007 audit procedures identified 12 information security control deficiencies, all of which relate to general controls. Specifically, the control deficiencies identified were in the areas of entitywide security program planning and management, access control, and system software. In the Limited Official Use Only report, we made 14 detailed recommendations to address these control deficiencies.

None of our findings pose significant risks to the FRB financial systems. As it relates to controls over financial reporting and compliance with applicable laws and regulations, the potential effect of such control deficiencies was mitigated by the FRBs and BPD. The FRBs mitigated the potential effect of such control deficiencies with physical security measures and a program of monitoring user and system activity, and BPD with compensating management and reconciliation controls that are designed to detect potential irregularities or improprieties in financial data or transactions.

The Board of Governors of the Federal Reserve System provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the Director of Reserve Bank Operations and Payment Systems stated that the FRBs have already taken action on many of the recommendations and the Board of Governors will continue to work with the FRBs to determine appropriate information security controls and compensating measures to address the remaining recommendations.

Background

Many of the FRBs provide fiscal agent services on behalf of BPD, which primarily consist of issuing, servicing, and redeeming Treasury securities held by the public and handling the related transfers of funds. In fiscal year 2007, the FRBs issued about $4.4 trillion in federal debt securities to the public, redeemed about $4.3 trillion of debt held by the public, and processed about $163 billion in interest payments on debt held by the public. FRBs use a number of financial systems to process debt-related transactions. Federal Reserve Information Technology Computing Centers

(FRIT) maintain and operate key financial systems on behalf of BPD and an array of financial and information systems to process and reconcile monies disbursed and collected on behalf of BPD. Detailed data initially processed at the FRBs are summarized and then forwarded electronically to BPD's data center for matching, verification, and posting to the general ledger.

Section 3544 (a)(1)(A) of Title 44, United States Code, delineates federal agency responsibilities for (1) information collected or maintained by or on behalf of an agency and (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Further, section 3544 (b) states that each agency shall develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Office of Management and Budget (OMB) Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* clarified that agency information security programs apply to all organizations which possess or use federal information—or which operate, use, or have access to federal information systems—on behalf of a federal agency. In addition, according to section 3544 (a)(1)(B) of Title 44, United States Code, federal agencies shall comply with information security standards developed by the National Institute of Standards and Technology (NIST).

Objectives, Scope, and Methodology

Our objectives were to evaluate the general and application information security controls over key financial management systems relevant to the Schedule of Federal Debt that are maintained and operated by the FRBs on behalf of BPD. We use a risk-based, rotation approach for testing general information security controls. Each general information security control area is subjected to a review, including testing, at least every 3 years. The general information security control areas we review are defined in the *Federal Information System Controls Audit Manual*.[4] Areas considered to be of higher risk are subject to more frequent review. Each key application is subjected to a review every year.

To evaluate general and application information security controls, we identified and reviewed information system general and application information security control policies and procedures, observed controls in operation, conducted tests of controls, and held discussions with officials at selected FRBs and FRIT to determine whether controls were adequately designed, implemented, and operating effectively.

The scope of our work for fiscal year 2007 as it relates to general information security controls included conducting a review of the general controls, which includes a review of the entitywide security program planning and management, access control,

[4]GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999).

application software development and change control, system software, segregation of duties, and service continuity. This effort included security configuration reviews of key Federal Reserve technical infrastructure components. We also reviewed results of security testing performed by staff within FRIT and FRB general audit functions.

Application information security control reviews were performed on six key FRB applications to determine whether the applications are designed to provide reasonable assurance 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 only to authorized users.

The evaluation and testing of certain information security controls were performed by the independent public accounting (IPA) firm of Cotton and Company, LLP. We agreed on the scope of the audit work, monitored the IPA firm's progress, and reviewed the related audit documentation to determine that the findings were adequately supported.

During our audit, we communicated our findings to the Board of Governors of the Federal Reserve System, who informed us that the FRBs have taken or plan to take corrective action to address the control deficiencies identified. We plan to follow up on these matters during our audit of the fiscal year 2008 Schedule of Federal Debt.

We performed our work at the FRB locations where the operations of the systems we reviewed are supported. Our work was performed from March 2007 through October 2007 in accordance with U.S. generally accepted government auditing standards. As noted above, we obtained agency comments on the detailed findings and recommendations in a draft of the separately issued Limited Official Use Only report. The Board of Governors of the Federal Reserve System's comments are summarized in the Agency Comments section of this report.

Assessment of FRBs' Information Security Controls

General information security controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General information security controls establish the environment in which application systems and controls operate. They include an entitywide security management program, access controls, system software controls, application software development and change controls,

segregation of duties, and service continuity. An effective general information security control environment helps (1) ensure that an adequate entitywide security management program 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 the event of a disaster or other unexpected interruption.

Our fiscal year 2007 testing identified opportunities to strengthen certain information security controls that support key financial systems maintained and operated by the FRBs on behalf of BPD relevant to the Schedule of Federal Debt. Specifically, our audit procedures identified 12 general information security control deficiencies. This included six control deficiencies related to entitywide security program planning and management, five control deficiencies related to access control, and one control deficiency related to system software.

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

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 access controls and physical access controls. The general information security control deficiencies that we identified relate to logical access controls. Logical access controls involve the use of computer hardware and software 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 access 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 computer resources.

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, file maintenance software, security software, data communications systems, and data management systems. Controls over access to and modifications of system software are essential to protect the overall integrity and reliability of information systems.

In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to FRB management and made 14 detailed recommendations.

None of our findings pose significant risks to the FRB financial systems. As it relates to controls over financial reporting and compliance with applicable laws and regulations, the potential effect of such control deficiencies was mitigated by the FRBs and BPD. The FRBs mitigated the potential effect of such control deficiencies with physical security measures and a program of monitoring user and system activity, and BPD with compensating management and reconciliation controls that are designed to detect potential irregularities or improprieties in financial data or transactions. Nevertheless, these findings warrant management's attention and action to limit the risk of unauthorized access, disclosure, loss, or impairment; modification of sensitive data and programs; and disruption of critical operations.

Conclusion

Our fiscal year 2007 audit identified 12 information security control deficiencies, all of which relate to general controls. For these identified control deficiencies, we are making 14 detailed recommendations. The Board of Governors of the Federal Reserve System informed us that the FRBs have taken or plan to take corrective action to address all of the control deficiencies we identified. We plan to follow up on the status of the FRBs' actions to address the identified control deficiencies as part of our fiscal year 2008 Schedule of Federal Debt audit.

Recommendation for Executive Action

We recommend that the Director of the Division of Reserve Bank Operations and Payment Systems direct the appropriate FRB officials to implement the 14 detailed recommendations set forth in the separately issued Limited Official Use Only version of this report.

Agency Comments

The Board of Governors of the Federal Reserve System provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the Director of Reserve Bank Operations and Payment Systems stated that the FRBs have already taken action on many of the recommendations and the Board of Governors will continue to work with the FRBs to determine appropriate information security controls and compensating measures to address the remaining recommendations. We plan to follow up on these matters during our audit of the fiscal year 2008 Schedule of Federal Debt.

- - - - -

In the separately issued Limited Official Use Only report, we requested a written statement on actions taken to address our recommendations not later than 60 days after the date of that report.

We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs; the Subcommittee on Financial Services and General Government, Senate Committee on Appropriations; the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Senate Committee on Homeland Security and Governmental Affairs; the House Committee on Oversight and Government Reform; the Subcommittee on Financial Services and General Government, House Committee on Appropriations; and the Subcommittee on Government Management, Organization, and Procurement, House Committee on Oversight and Government Reform. We are also sending copies of this report to the Chairman of the Board of Governors of the Federal Reserve System, the Fiscal Assistant Secretary of the Treasury, and the Director of the Office of Management and Budget. Copies will also be made available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-3406 or engelg@gao.gov. Other key contributors to this assignment were Jeffrey L. Knott and Dawn B. Simpson, Assistant Directors; Dean D. Carpenter; Mary T. Marshall; and Zsaroq R. Powe.

Sincerely yours,

Gary T. Engel
Director
Financial Management and Assurance

(198518)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548