



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 29, 2009

Stephen R. Malphrus
Staff Director for Management
Board of Governors of the Federal
Reserve System

Subject: *Federal Reserve Banks: Areas for Improvement in Information Security Controls*

Dear Mr. Malphrus:

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, 2008 and 2007.² 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 (FRB) on behalf of the Department of the Treasury's (Treasury) BPD relevant to the Schedule of Federal Debt.

As we reported in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2008 and 2007, 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, 2008, 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 deficiencies involving information security controls that we do not consider to be significant deficiencies.³ With regard to 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

¹31 U.S.C. § 331(e).

²GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2008 and 2007 Schedules of Federal Debt*, GAO-09-44 (Washington, D.C.: Nov. 7, 2008).

³A 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.

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 control deficiencies 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 we identified during our fiscal year 2008 testing of the general and application information security controls over key financial systems maintained and operated by the FRBs relevant to BPD's Schedule of Federal Debt. This report also includes the results of our follow-up on the status of FRB's corrective actions to address recommendations that were contained in our prior year's report. In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to FRB management.

Results

Our fiscal year 2008 audit procedures identified two new general information security control deficiencies, related to entitywide security program planning and management, and system software. In the Limited Official Use Only report, we made two recommendations to address these control deficiencies.

None of the control deficiencies we identified represented significant risks to the key financial systems maintained and operated by the FRBs on behalf of BPD. With regard to 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 misstatements in the Schedule of Federal Debt. 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.

During our follow-up on the status of FRBs' corrective actions to address 14 open recommendations related to general information security control deficiencies identified in our prior year's audit, we determined the following:

- As of September 30, 2008, corrective action on 5 of the 14 recommendations was completed.
- Corrective action was in progress as of September 30, 2008, on almost all of the nine remaining open recommendations. Five of these recommendations related to entitywide security program planning and management, three related to access control, and one related to system software. Although FRB management has made progress in addressing the remaining nine general information security control deficiencies, additional actions are still needed.

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 are taking corrective action to implement the two new recommendations resulting from our fiscal year 2008 audit procedures and have completed corrective action on seven of the nine open recommendations from our prior year's report. Of the two remaining recommendations, the Director indicated that one is scheduled to be addressed by the third quarter 2009, and the other one will necessitate direction from Treasury to implement corrective action.

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 2008, the FRBs issued about \$5.5 trillion in federal debt securities to the public, redeemed about \$4.7 trillion of debt held by the public, and processed about \$171 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 other 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.

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.

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.

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.

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).

Conclusion

FRB has made progress in addressing the open information security control recommendations from our prior year's report and is taking corrective action to address but has not yet completed all required actions on the remaining unresolved control deficiencies.

Our fiscal year 2008 audit also identified two new general information security control deficiencies related to entitywide security program planning and management, and system software. For these identified control deficiencies, we are making two recommendations.

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 two detailed recommendations set forth in the separately issued Limited Official Use Only report.

Agency Comments and Our Evaluation

The Board of Governors of the Federal Reserve System provided comments on the detailed financial and recommendations in the Limited Official Use Only version. In those comments, the Director of Reserve Bank Operations and Payment Systems stated that the FRBs are taking corrective action to implement the two new recommendations resulting from our fiscal year 2008 audit procedures and have

completed corrective action on seven of the nine open recommendations from our prior year's report. Of the two remaining recommendations, the Director indicated that one is scheduled to be addressed by the third quarter 2009, and the other one will necessitate direction from Treasury to implement corrective action. We plan to follow up on corrective actions taken for these matters during our audit of the fiscal year 2009 Schedule of Federal Debt.

Objectives, Scope, and Methodology

Our objectives were to evaluate the general and application information security controls over key financial management systems maintained and operated by the FRBs on behalf of BPD that are relevant to the Schedule of Federal Debt, and to determine the status of corrective actions taken in response to the recommendations in our prior year's report. We use a risk-based, rotation approach for testing general information security controls. Each general information security control area is subjected to a more detailed 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 FRB's 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 2008 as it relates to general information security controls included following up on open recommendations from our prior year's report, and reviewing the entitywide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity for an application implemented in April 2008. For the other applications, we reviewed access control, system software, and segregation of duties. 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 seven 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;

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

- 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, including the follow-up on the status of FRB's corrective actions to address open recommendations in our prior year's report, 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.


We performed our work at the FRB locations where the operations of the systems we reviewed are supported. Our work was performed from March 2008 through October 2008 in accordance with U.S. generally accepted government auditing standards. During the course of our work, we communicated our findings to the Board of Governors of the Federal Reserve System. 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 and Our Evaluation section of this report.

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 interested congressional committees, 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. In addition, this report is available at no charge on the GAO 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. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are Jeffrey L. Knott and Dawn B. Simpson, Assistant Directors; Dean D. Carpenter; and Zsaroq R. Powe.

Sincerely yours,

A handwritten signature in black ink that reads "Gary T. Engel". The signature is written in a cursive style with a large initial "G" and "E".

Gary T. Engel
Director
Financial Management and Assurance

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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