GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 21, 2010

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, 2009 and 2008.[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, 2009 and 2008, we concluded that BPD maintained, in all material respects, effective internal control over financial reporting relevant to the Schedule of Federal Debt as of September 30, 2009, that provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt would be prevented or detected and corrected on a timely basis. However, we identified information security deficiencies affecting internal control over financial reporting, which, while we do not consider them to be collectively either a material weakness or significant deficiency, nevertheless warrant FRB management's attention and action.[3]

---

[1]31 U.S.C. § 331(e).
[2]GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2009 and 2008 Schedules of Federal Debt*, GAO-10-88 (Washington, D.C.: Nov. 10, 2009).
[3]A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A deficiency in internal control 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 and correct misstatements on a timely basis.

This report presents the control deficiencies we identified during our fiscal year 2009 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 information security control related recommendations contained in our prior years' audit reports and open as of September 30, 2008. 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 2009 audit procedures identified four new general information security control deficiencies related to security management and access controls. We made five 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. The potential effect of such control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRB's physical security measures and a program of monitoring user and system activity, and BPD's compensating management and reconciliation controls designed to detect potential misstatements in the Schedule of Federal Debt.

In addition, during our fiscal year 2009 follow-up on the status of FRB's corrective actions to address 11 open recommendations related to general information security control deficiencies identified in our prior years' audits, we determined that as of September 30, 2009, corrective action on 8 of the 11 recommendations was completed, while corrective action was in progress on the 3 remaining open recommendations, which related to security management.

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 agency takes control deficiencies, and actions to address them, seriously. The Director further commented that three deficiencies have already been addressed or remediated, and that the remainder have corrective actions planned or in progress.

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 2009, the FRBs issued about $8.9 trillion in federal debt securities to the public, redeemed about $7.1 trillion of debt held by the public, and processed about $166 billion in interest payments on debt held by the public. FRBs use a number of financial systems to process debt-related transactions. The Federal Reserve Information Technology Computing Centers maintain and operate key financial systems to process and reconcile moneys 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) provides 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 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, section 3544(a)(1)(B) of Title 44, United States Code, requires federal agencies to comply with information security standards developed by the National Institute of Standards and Technology.

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 years' reports for which actions were not complete as of September 30, 2008. Our evaluation of the general and application information security controls was conducted using the *Federal Information System Controls Audit Manual.*[4]

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 FRB data centers to determine whether controls were adequately designed, implemented, and operating effectively.

The scope of our general information security controls work for fiscal year 2009 included following up on open recommendations from our prior years' reports and a risk-based approach to testing all five general control areas in the current year. Based on this approach, our testing focused primarily on access controls and configuration management and, to a lesser extent, on the other areas of security management, segregation of duties, and contingency planning. In addition, we performed security configuration reviews of key Federal Reserve technical infrastructure components. We also reviewed results of security testing performed by FRB Richmond General Audit.

[4]GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

We performed application information security control reviews on four key FRB applications to determine whether the applications were designed to provide reasonable assurance that

- all transactions that occurred were input into the system, accepted for processing, processed once and only once by the system, and properly included in output;
- transactions were properly recorded in the proper period, key data elements input for transactions were accurate, data elements were processed accurately by applications that produce reliable results, and output was accurate;
- all recorded transactions actually occurred, related to the organization, and were properly approved in accordance with management's authorization, and output contained only valid data;
- application data and reports and other output were protected against unauthorized access; and
- application data and reports and other relevant business information were readily available to users when needed.

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 from our prior years' reports, 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 the course of our work, we communicated our findings to the Board of Governors of the Federal Reserve System. We plan to follow up to determine the status of corrective actions taken for matters open as of September 30, 2009, during our audit of the fiscal year 2010 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 February 2009 through October 2009 in accordance with U.S. generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

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.

Assessment of FRB's 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 security management, access controls, configuration

management, segregation of duties, and contingency planning. An effective general information security control environment (1) provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls to ensure that an adequate security management program is in place; (2) limits or detects access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (3) prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended; (4) includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and (5) protects critical and sensitive data, and provides for critical operations to continue without disruption or be promptly resumed when unexpected events occur.

Our fiscal year 2009 testing identified opportunities to strengthen certain information security controls that support key financial systems maintained and operated by the FRBs relevant to BPD's Schedule of Federal Debt. Specifically, our audit procedures identified four new general information security control deficiencies. This consisted of two control deficiencies related to security management and two control deficiencies related to access controls.

An entitywide information security management program is important because it provides the foundation for an effective security control structure. The security management program establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans, including system and application-specific procedures and controls, implement the entitywide policy.

Access controls are important because they limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include logical access controls and physical access controls. The new access control deficiencies we identified related to logical access controls. Logical access controls require users to authenticate themselves through the use of secret passwords or other identifiers, and limit the files and other resources that authenticated users can access and the actions that they can execute.

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

In addition, during our fiscal year 2009 follow-up on the status of FRB's corrective actions to address 11 open recommendations related to information security control deficiencies we identified in our prior years' audits, we determined that as of September 30, 2009, corrective action on 8 of the 11 recommendations was completed, while corrective action was in progress on the 3 remaining open recommendations, which related to security management. Although FRB

management has made progress in addressing the remaining 3 general information security control deficiencies, additional actions are still needed.

None of the control deficiencies we identified represented significant risks to the financial systems maintained and operated by the FRBs on behalf of BPD. The potential effect of such control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRB's physical security measures and a program of monitoring user and system activity, and BPD's compensating management and reconciliation controls designed to detect potential misstatements in the Schedule of Federal Debt. Nevertheless, these deficiencies warrant management's attention and action to limit the risk of unauthorized access, loss, or disclosure; modification of sensitive data and programs; and disruption of critical operations.

Conclusion

FRB has made significant progress in addressing the open information security control recommendations from our prior years' audits, and while actions are still needed in three control areas, it has corrective actions underway or planned. Our fiscal year 2009 audit also identified four new general information security control deficiencies related to security management and access controls.

Recommendations 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 five new detailed recommendations presented 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 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 agency takes control deficiencies, and actions to address them, seriously. Specifically, it commented that of the eight recommendations open as of September 30, 2009, three have been completely resolved and corrective actions for the remaining five are planned or in progress. The Director also stated that the FRBs intend to implement corrective action for four of the five remaining findings by September 2010, and actions to address the other finding over the next several years as part of a transition to a new information security program. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2010 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 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 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. 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 include Jeffrey L. Knott and Dawn B. Simpson, Assistant Directors; Dean D. Carpenter; and Nicole N. Jarvis.

Sincerely yours,

Gary T. Engel
Director
Financial Management and Assurance

(198606)

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