United States Government Accountability Office
Washington, DC 20548

April 11, 2012

Dave Caperton
Special Counsel, Legal Division
Board of Governors of the Federal
Reserve System

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

Dear Mr. Caperton:

In connection with fulfilling our requirement to audit the consolidated 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, 2011 and 2010.[2] As part of these audits, we performed a review of information systems 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, 2011 and 2010, 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, 2011, 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 systems deficiencies affecting internal control over financial reporting, which, while we do not consider

[1]31 U.S.C. § 331(e)(2). As a bureau within the Department of the Treasury, federal debt and related activity and balances are also significant to the consolidated financial statements of Treasury (see 31 U.S.C. § 3515(b)).

[2]GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2011 and 2010 Schedules of Federal Debt,* GAO-12-164 (Washington, D.C.: Nov. 8, 2011).

them to be collectively either a material weakness or significant deficiency, nevertheless warrant the attention and action of management.[3]

With regard to key financial systems maintained and operated by the FRBs on behalf of BPD, we did not identify any new deficiencies in information systems controls that had a consequential effect on financial reporting relevant to the Schedule of Federal Debt during our fiscal year 2011 audit. In a separately issued Limited Official Use Only report, we communicated to FRB management detailed information regarding the results of our follow up on the status of FRBs' corrective actions to address information systems control-related recommendations contained in our prior years' reports and open as of September 30, 2010.

Results in Brief

During our fiscal year 2011 follow up on the status of FRBs' corrective actions to address information systems control-related recommendations contained in our prior years' reports and open as of September 30, 2010, we determined that corrective action was in progress for each of the three open recommendations related to security management and access controls. The potential effect of these continuing control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRBs' 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.

The Director of Reserve Bank Operations and Payments Systems on behalf of the Board of Governors of the Federal Reserve System provided comments on the detailed information regarding the results of our follow up on the status of FRBs' corrective actions in the separately issued Limited Official Use Only report. In those comments, the Director stated that the agency takes control deficiencies seriously and that FRB management continues to make progress towards addressing the three open recommendations. The Director further commented that one of the deficiencies has already been addressed, and that corrective actions for the two remaining open recommendations from our prior years' reports are planned or in progress.

Background

Treasury is authorized by Congress to borrow money backed by the full faith and credit of the United States to fund federal operations. Treasury is responsible for prescribing the debt instruments and otherwise limiting and restricting the amount and composition of the debt. BPD, an organizational entity within the Fiscal Service

[3]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 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 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.

of the Treasury, is responsible for issuing and redeeming debt instruments, paying interest to investors, and accounting for the resulting debt.

Many of the FRBs provide fiscal agent services on behalf of BPD. Such services primarily consist of issuing, servicing, and redeeming Treasury securities held by the public and handling the related transfers of funds. In fiscal year 2011, the FRBs issued about $7.8 trillion in federal debt securities to the public, redeemed about $6.7 trillion of debt held by the public, and processed about $210 billion in interest payments on debt held by the public. FRBs use a number of key financial systems to process debt-related transactions. The Federal Reserve Information Technology Computing Centers maintain and operate key financial systems to process and reconcile funds 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-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, clarifies that agency information security programs apply to all organizations that possess or use federal information—or that 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 (NIST).

General information systems controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General information systems controls establish the environment in which the application systems and controls operate. They include the five *Federal Information System Controls Audit Manual* (FISCAM)[4] general control areas—security management, access controls, configuration management, segregation of duties, and contingency planning. An effective general information systems 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 (security management); (2) limits or detects access to computer resources, such as data, programs, equipment, and facilities, thereby protecting them against unauthorized modification, loss, and disclosure (access controls); (3) prevents unauthorized changes to information system resources, such as software programs and hardware configurations, and provides reasonable

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

assurance that systems are configured and operating securely and as intended (configuration management); (4) includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations (segregation of duties); and (5) protects critical and sensitive data, and provides for critical operations to continue without disruption or be promptly resumed when unexpected events occur (contingency planning).

Objectives, Scope, and Methodology

Our objectives were to evaluate information systems controls over key financial 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 FRBs' corrective actions to address information systems control-related recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2010. Our evaluation of information systems controls was conducted using FISCAM.

To evaluate information systems controls, we identified and reviewed FRBs' information systems 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 systems controls work for fiscal year 2011 included (1) following up on open recommendations from our prior years' reports and (2) using a risk-based approach to testing the five FISCAM general control areas related to the systems in which the applications operate and other critical control points in the systems or networks that could impact the effectiveness of the information systems controls at the relevant FRBs in the current year. In addition, we assessed software and network security by reviewing vulnerability scans and penetration testing performed by the FRBs over key financial systems maintained and operated by the FRBs on behalf of BPD that are relevant to the Schedule of Federal Debt. We also reviewed results of general control testing specific to physical security access controls, contingency planning, and security management performed by FRB Richmond General Audit and access control testing specific to a key FRB application performed by FRB Philadelphia General Audit relevant to our fiscal year 2011 audit.

We determined whether relevant application controls were appropriately designed and implemented, and then performed tests to determine whether the application controls were operating effectively. We reviewed four key FRB applications relevant to the Schedule of Federal Debt to determine whether the application controls were designed and operating effectively 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 independent public accounting (IPA) firm of Cotton and Company LLP evaluated and tested certain FRBs' information systems controls, including the follow up on the status of FRBs' corrective actions during fiscal year 2011 to address open recommendations from our prior years' reports. 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 firm's 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, 2011, during our audit of the fiscal year 2012 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 2011 through October 2011 in accordance with U.S. generally accepted government auditing standards. We believe that our audit provided a reasonable basis for our conclusions in this report.

As noted above, we obtained agency comments on the detailed information regarding the results of our follow up on the status of FRBs' corrective actions in 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 FRBs' Information Systems Controls

With regard to key financial systems maintained and operated by the FRBs on behalf of BPD, we did not identify any new deficiencies in information systems controls that had a consequential effect on financial reporting relevant to the Schedule of Federal Debt during our fiscal year 2011 audit. However, our fiscal year 2011 follow up on the status of actions taken to address previously identified, but unresolved, general information systems control deficiencies as of September 30, 2010, found that, although FRB management made progress, additional actions are needed in all three areas related to security management and access controls. The potential effect of these continuing control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRBs' 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 a separately issued Limited Official Use Only report, we communicated to FRB management detailed information regarding the results of our follow up on the status of FRBs' corrective actions to address information systems control-related recommendations contained in our prior years' reports and open as of September 30, 2010.

Conclusion

While the FRBs have corrective actions under way or planned, additional actions are needed to fully address the open information systems control recommendations from our prior years' audits in three control areas. Until these information systems control deficiencies are fully addressed, there will be an increased risk that internal control deficiencies may exist and remain unidentified and an increased risk of unauthorized access, loss, or disclosure; modification of sensitive data and programs; and disruption of critical operations. We will follow up to determine the status of FRBs' actions taken in response to these open recommendations during our audit of the fiscal year 2012 Schedule of Federal Debt.

Agency Comments and Our Evaluation

In commenting on a draft of this report, the Director of Reserve Bank Operations and Payment Systems on behalf of the Board of Governors of the Federal Reserve System stated that the agency takes control deficiencies seriously and that FRB management continues to make progress towards addressing the three open recommendations. Specifically, the Director commented that one of the deficiencies has already been addressed, and that corrective actions for the two remaining open recommendations from our prior years' reports are planned or in progress. The Director also stated that the FRBs intend to implement corrective actions for one of the two remaining findings by September 2012 as part of a transition to a new information security program, and complete actions to address the other finding in 2013. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2012 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 Acting Director of the Office of Management and Budget. In addition, this report is available at no charge on the GAO website 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; William B. Cook; George C. Kovachick; Nicole M. McGuire; and Seong Bin Park.

Sincerely yours,

Gary T. Engel
Director
Financial Management and Assurance

(198698)