



United States Government Accountability Office  
Washington, DC 20548

May 9, 2013

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,<sup>1</sup> 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, 2012 and 2011.<sup>2</sup> 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 (Treasury) 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, 2012 and 2011, 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, 2012, 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 them individually or collectively to be either material weaknesses or significant deficiencies, nevertheless warrant the attention and action of management.<sup>3</sup>

This report presents the deficiencies we identified during our fiscal year 2012 testing of information systems controls over key financial systems maintained and operated by FRBs

<sup>1</sup>31 U.S.C. § 331(e)(2). Federal debt and related activity and balances managed by BPD during fiscal years 2012 and 2011 were also significant to the consolidated financial statements of the Department of the Treasury (see 31 U.S.C. § 3515(b)).

<sup>2</sup>GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2012 and 2011 Schedules of Federal Debt*, GAO-13-114 (Washington, D.C.: Nov. 8, 2012).

<sup>3</sup>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 a 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.

on behalf of Treasury relevant to the Schedule of Federal Debt. This report also includes the results of our follow-up on the status of FRBs' corrective actions to address information systems control-related deficiencies and associated recommendations contained in our prior years' reports and open as of September 30, 2011. In a separately issued Limited Official Use Only report, we communicated to FRB management detailed information regarding our findings and related recommendations.

## **Results in Brief**

During our fiscal year 2012 audit, we identified two new general information systems control deficiencies related to security management. 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 financial systems maintained and operated by FRBs on behalf of Treasury. The potential effect of these deficiencies on the Schedule of Federal Debt financial reporting 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 of the Schedule of Federal Debt.

In addition, during our follow-up on the status of FRBs' corrective actions to address information systems control-related deficiencies and associated recommendations contained in our prior years' reports and open as of September 30, 2011, we determined that corrective action was complete for two of the three open recommendations and corrective action was in progress for the remaining open recommendation related to access controls.

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 findings and recommendations 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 is addressing the two new general information systems control deficiencies. The Director further commented that corrective action for the remaining open recommendation from our prior years' reports is 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. Treasury is also responsible for issuing and redeeming debt instruments, paying interest to investors, and accounting for the resulting debt.

Many FRBs provide fiscal agent services on behalf of Treasury. 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 2012, FRBs issued about \$7.6 trillion in federal debt securities to the public, redeemed about \$6.4 trillion of debt held by the public, and processed about \$218 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 Treasury. Detailed data initially processed at FRBs are summarized and then forwarded electronically to the appropriate Treasury 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 providing information security protections 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 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-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, clarifies that agency information security programs apply to all organizations (sources) that process, store, or transmit federal information—or that operate, use, or have access to federal information systems (whether automated or manual)—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.

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 general control areas—security management, access controls, configuration management, segregation of duties, and contingency planning.<sup>4</sup> 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 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 FRBs on behalf of Treasury that are relevant to the Schedule of Federal Debt, and to determine the status of FRBs' corrective actions to address information systems control-related deficiencies and associated recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2011. Our evaluation of information systems controls was conducted using the Federal Information System Controls Audit Manual.<sup>5</sup>

---

<sup>4</sup>GAO, *Government Auditing Standards*, GAO-07-731G (Washington, D.C.: July 2007). The July 2007 revision of *Government Auditing Standards* has been superseded by the December 2011 revision, GAO, *Government Auditing Standards*, GAO-12-331G (Washington, D.C.: December 2011). However, the July 2007 revision is cited here because this version was effective for our audit of the Schedules of Federal Debt Managed by BPD for the fiscal years ended September 30, 2012 and 2011.

<sup>5</sup>GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

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 2012 included (1) following up on open recommendations from our prior years' reports and (2) using a risk-based approach to testing the five general control areas related to the systems in which the applications operate and other critical control points in the systems or networks that could have an impact on 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 over key financial systems maintained and operated by FRBs on behalf of Treasury that are relevant to the Schedule of Federal Debt. We also reviewed results of general control testing specific to contingency planning performed by FRB Richmond General Audit<sup>6</sup> relevant to our fiscal year 2012 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, were 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 & Company LLP evaluated and tested certain FRBs' information systems controls, including the follow-up on the status of FRBs' corrective actions during fiscal year 2012 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 whether 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, 2012, during our audit of the fiscal year 2013 Schedule of Federal Debt.

We performed our work 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.

---

<sup>6</sup>Each FRB has an internal audit governance structure (referred to in this report as General Audit) that reports to the FRB's Board of Directors.

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 FRBs' Information Systems Controls**

During our fiscal year 2012 testing, we identified opportunities to strengthen certain information systems controls that support key financial systems maintained and operated by FRBs on behalf of Treasury relevant to the Schedule of Federal Debt. Specifically, we identified two new general information systems control deficiencies related to security management. In addition, during fiscal year 2012, the Board of Governors of the Federal Reserve System identified a general information systems control deficiency related to security management. We considered this deficiency, along with those deficiencies identified by us, in determining that there was not a material weakness or significant deficiency in internal control over financial reporting relevant to the Schedule of Federal Debt.

Security management is important because it is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. Effectively designed and implemented security management programs establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed security management program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or 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.

In a separately issued Limited Official Use Only report, we communicated to FRB management detailed information regarding the two new general information systems control deficiencies and made two recommendations to address these control deficiencies.

In addition, our fiscal year 2012 follow-up on the status of actions taken by FRBs to address previously identified, but unresolved, general information systems control deficiencies as of September 30, 2011, found that corrective action was complete for two of the three open recommendations and corrective action was in progress for the remaining open recommendation related to access controls.

None of the control deficiencies we identified represented significant risks to the financial systems maintained and operated by FRBs on behalf of Treasury. The potential effect of these control deficiencies on the Schedule of Federal Debt financial reporting 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 of the Schedule of Federal Debt. Nevertheless, these deficiencies increase the risk of unauthorized access, loss, modification, or disclosure of sensitive data and programs and disruption of critical operations and, therefore, warrant the attention and action of management.

### **Agency Comments and Our Evaluation**

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 findings and

recommendations 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 is addressing the two new general information systems control deficiencies. The Director further commented that corrective action for the remaining open recommendation from our prior years' reports is in progress. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2013 Schedule of Federal Debt.

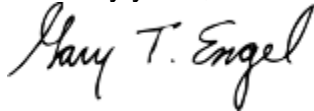
- - - - -

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 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](mailto: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 members who made major contributions to this report include Dianne D. Guensberg, Jeffrey L. Knott, and Dawn B. Simpson (Assistant Directors); Nicole M. Burkart; Bruce E. Cain; Dean D. Carpenter; and Seong Bin Park.

Sincerely yours,



Gary T. Engel  
Director  
Financial Management and Assurance

(198720)

---

---

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 website ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://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 website, <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.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@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](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

