



441 G St. N.W.
Washington, DC 20548

April 3, 2015

Mr. David Caperton
Special Counsel, Legal Division
Board of Governors of the Federal
Reserve System

Management Report: Areas for Improvement in the Federal Reserve Banks' Information Systems Controls

Dear Mr. Caperton:

In connection with our audit of 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 Fiscal Service (Fiscal Service) for the fiscal years ended September 30, 2014, and 2013.² 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 (Treasury) relevant to the Schedule of Federal Debt.

As we reported in connection with our audits of the Schedules of Federal Debt for the fiscal years ended September 30, 2014, and 2013, Fiscal Service maintained, in all material respects, effective internal control over financial reporting relevant to the Schedule of Federal Debt as of September 30, 2014, based on criteria established under 31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act (FMFIA). Those controls provided reasonable assurance that misstatements material in relation to the Schedule of Federal Debt would be prevented, or detected and corrected, on a timely basis. While we identified control deficiencies relating to information systems controls relevant to the Schedule of Federal Debt, we do not consider them individually or collectively to be material weaknesses or significant deficiencies.³ Nevertheless, these control deficiencies warrant the attention and action of management.

¹31 U.S.C. § 331(e)(2). Federal debt and related activity and balances managed by the Bureau of the Fiscal Service during fiscal years 2014 and 2013 were also significant to the consolidated financial statements of the Department of the Treasury (see 31 U.S.C. § 3515(b)).

²GAO, *Financial Audit: Bureau of the Fiscal Service's Fiscal Years 2014 and 2013 Schedules of Federal Debt*, GAO-15-157 (Washington, D.C.: Nov. 10, 2014).

³A 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.

With regard to key financial systems maintained and operated by the FRBs on behalf of Treasury during fiscal year 2014, we identified and communicated to FRB management certain new internal control deficiencies, but did not consider them significant enough to include in this report. 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, 2013.

Results in Brief

During our fiscal year 2014 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 that were open as of September 30, 2013, we determined that corrective action was complete for four of the six open recommendations and corrective actions were in progress for the remaining two open recommendations related to security management.

The potential effect of these continuing control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRBs' program of monitoring user and system activity and Fiscal Service's compensating management and reconciliation controls designed to detect potential misstatements of 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 has since addressed one of the remaining open recommendations and corrective actions are in progress for the remaining recommendation.

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 2014, FRBs issued about \$7.2 trillion in federal debt securities to the public, redeemed about \$6.6 trillion of debt held by the public, and processed about \$229 billion in interest payments on debt held by the public. FRBs use a number of key financial systems to process debt-related transactions. Federal Reserve Information Technology (FRIT) 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 Fiscal Service's data center for matching, verification, and posting to Fiscal Service's general ledger.

During the period of our audit, section 3544(a)(1)(A) of Title 44, United States Code, delineated 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.⁴ In addition, section 3544(a)(1)(B) requires federal agencies to comply with information security standards developed by the National Institute of Standards and Technology. Further, section 3544(b) provides that each agency shall develop, document, and implement an agency-wide 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-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (November 18, 2013), 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.

Information systems general controls are the structure, policies, and procedures that apply to an entity's overall computer operations. Information systems general controls establish the environment in which the application systems and controls operate. They include five general control areas—security management, access controls, configuration management, segregation of duties, and contingency planning.⁵ An effective information systems general 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, 2013. Our evaluation of information systems controls was conducted using the *Federal Information System Controls Audit Manual*.⁶ This work was performed in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2014, and 2013, for the purpose of

⁴Section 3544 was enacted as part of the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). The recent Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), amended chapter 35 of Title 44, U.S. Code, and largely superseded the 2002 act, to include repealing section 3544 and replacing it with a new section 3554. However, the 2002 act was the law in effect during the period in which we conducted this audit.

⁵GAO, *Government Auditing Standards: 2011 Revision*, GAO-12-331G (Washington, D.C.: December 2011).

⁶GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

supporting our opinion on Fiscal Service's internal control over financial reporting relevant to the Schedule of Federal Debt.

To evaluate information systems controls, we identified and reviewed FRBs' information systems control policies and procedures; observed controls in operation; conducted tests of controls; reviewed the independence and qualifications of FRB Richmond General Audit,⁷ which has been assigned audit responsibility for FRIT; reviewed the independence and qualifications of FRB Boston General Audit; and held discussions with officials at selected FRBs to determine whether controls were adequately designed, implemented, and operating effectively.

The scope of our information systems general controls work for fiscal year 2014 included (1) following up on open recommendations from our prior years' reports; (2) using a risk-based approach to test 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 as they relate to financial reporting in the current year relevant to the Schedule of Federal Debt; (3) assessing 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; (4) reviewing results of general control testing specific to contingency planning, as well as mainframe general controls related to a key FRB system, performed by FRB Richmond General Audit relevant to our fiscal year 2014 audit; and (5) reviewing results of control testing specific to a key FRB system performed by FRB Boston General Audit relevant to our fiscal year 2014 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 two 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

- 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 produced reliable results, and output was accurate;
- 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.

GAO used an independent public accounting (IPA) firm, under contract, to assist in information systems testing, including the follow-up on the status of FRBs' corrective actions during fiscal year 2014 to address open recommendations from our prior years' reports. We agreed on the scope of the IPA's work, monitored and reviewed all aspects of its work, and determined that

⁷Each FRB has an internal audit governance structure (referred to in this report as General Audit) that reports to the FRBs' board of directors.

the work was sufficient to satisfy our audit objectives. Other work was developed wholly by GAO or in collaboration with the IPA.

During the course of our work, we communicated our findings to the Board of Governors of the Federal Reserve System, Richmond General Audit, Boston General Audit, New York General Audit, and FRIT. We plan to follow up to determine the status of corrective actions taken for matters open as of September 30, 2014, during our audit of the fiscal year 2015 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.

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 section of this report.

Additional Actions to Address Previously Identified Information Systems General Control Deficiencies

Our fiscal year 2014 follow-up on the status of actions taken by FRBs to address previously identified, but unresolved, information systems general control deficiencies as of September 30, 2013, found that corrective action was complete for four of the six open recommendations and corrective actions were in progress for the remaining two open recommendations. Specifically, the FRBs completed corrective actions for all open recommendations related to access controls and configuration management. However, FRB management needs to take additional actions to address remaining deficiencies in two areas related to security management.

The potential effect of these continuing control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRBs' program of monitoring user and system activity and Fiscal Service's compensating management and reconciliation controls designed to detect potential misstatements of 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, 2013.

Conclusions

While the FRBs had corrective actions under way as of September 30, 2014, additional actions are needed to fully address the two open information systems control-related deficiencies and associated recommendations concerning security management from our prior years' audits. Until these continuing information systems control deficiencies are fully addressed, management's ability to adequately assess all relevant controls expected to be incorporated into systems and make appropriate conclusions about the security status of such systems will be impaired. We will follow up to determine the status of actions taken in response to these information systems control-related deficiencies and associated recommendations during our audit of the fiscal year 2015 Schedule of Federal Debt.

Agency Comments

The Director of Reserve Bank Operations and Payment 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 has since addressed one of the remaining open recommendations and corrective actions are in progress for the remaining recommendation. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2015 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, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff 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 members who made major contributions to this report include Nicole M. Burkart, Dianne D. Guensberg, David B. Hayes, and Jeffrey L. Knott (assistant directors); Mickie E. Gray; J. Andrew Long; and Ivy Wu.

Sincerely yours,



Gary T. Engel
Director
Financial Management and Assurance

(198743)