U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Accessible Version

June 6, 2016

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, 2015, and 2014.[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, 2015, and 2014, Fiscal Service maintained, in all material respects, effective internal control over financial reporting relevant to the Schedule of Federal Debt as of September 30, 2015, based on criteria established under 31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act. 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. This report presents the deficiencies we identified during our fiscal year 2015 testing of information systems controls over key financial systems maintained and operated by FRBs on behalf of

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

[2]GAO, *Financial Audit: Bureau of the Fiscal Service's Fiscal Years 2015 and 2014 Schedules of Federal Debt*, GAO-16-160 (Washington, D.C.: Nov. 13, 2015).

[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 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.

Treasury that are 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 that were open as of September 30, 2014. 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 2015 audit, we identified three new information systems general control deficiencies related to security management and configuration management. In the Limited Official Use Only report, we made four recommendations to address these control deficiencies.

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 that were open as of September 30, 2014, we determined that corrective action was complete for one of the two open recommendations and corrective action was in progress for the remaining open recommendation related to security management.

These control deficiencies limit management's ability to determine whether controls are adequate to address security risks and meet the security requirements of information systems and reasonably assure that information technology products are properly configured to minimize security risks and, therefore, warrant the attention and action of management. The potential effect of these new and continuing deficiencies on the Schedule of Federal Debt financial reporting for fiscal year 2015 was mitigated primarily 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 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 is taking corrective action to address the three new information systems general control deficiencies. The Director further commented that FRB management has since addressed the remaining open recommendation from our prior year's report. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2016 Schedule of Federal Debt.

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 2015, FRBs issued about $6.9 trillion in federal debt securities to the public, redeemed about $6.4 trillion of debt held by the public, and processed about $237 billion in interest payments on debt held by the public. FRBs use a number of key financial systems to process debt-related transactions. National Information Technology

(National IT), comprising Federal Reserve Information Technology (FRIT)[4] and National IT operators, maintains and operates 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 Treasury's data center for matching, verification, and posting to Fiscal Service's general ledger.

During the period of our audit, federal law required each federal agency to provide information security protections for (1) information collected or maintained by or on behalf of the agency and (2) information systems used or operated by the agency or by a contractor or other organization on the agency's behalf.[5] In addition, federal agencies were required to comply with information security standards developed by the National Institute of Standards and Technology. Further, each agency was required to 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 (OMB) Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (issued October 3, 2014), 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.[6]

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.[7] 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

[4]FRIT is a National IT service provider that provides operational and project services, enterprise information technology architecture and standards services, and enterprise information security policy and assurance services throughout the Federal Reserve System.

[5]During the period of our audit, federal agency information security responsibilities were provided by two laws: the Federal Information Security Management Act of 2002 (FISMA 2002), Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002), *codified* at 44 U.S.C. §§ 3541, *et. seq*., and the Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), *codified* at 44 U.S.C. §§ 3551, *et. seq*. FISMA 2014 largely superseded the very similar FISMA 2002, but it retained virtually all of the federal agency requirements previously established by FISMA 2002. In particular, the federal agency responsibilities noted in this report were codified at 44 U.S.C. § 3544 for FISMA 2002 and are codified at 44 U.S.C. § 3554 for FISMA 2014.

[6]M-15-01 states that unless specifically updated or otherwise modified, it incorporates by reference the information conveyed in the Frequently Asked Questions (FAQ) and definitions from the guidance issued in 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* (issued November 18, 2013). This clarifying statement is included in the FAQs in M-14-04 and incorporated by reference in M-15-01.

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

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, 2014. Our evaluation of information systems controls was conducted using the *Federal Information System Controls Audit Manual*.[8] This work was performed in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2015, and 2014, for the purpose of 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,[9] which has been assigned audit responsibility for FRIT; 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 2015 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; and (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 2015 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

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

[9]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.

- 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 2015 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 the work was sufficient to satisfy our audit objectives.

During the course of our work, we communicated our results to the Board of Governors of the Federal Reserve System, as well as other Federal Reserve stakeholders with audit or operational responsibilities pertaining to the information systems general controls and relevant application controls we tested. We plan to follow up to determine the status of corrective actions taken for matters open as of September 30, 2015, during our audit of the fiscal year 2016 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.

Assessment of FRBs' Information Systems General Controls

During our fiscal year 2015 audit, we identified three new information systems general control deficiencies. One of these deficiencies related to security management and two related to configuration management.

Security management 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 a continuous cycle of activity for managing risk, developing and implementing effective security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. 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.

Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. Effectively designed and implemented configuration management controls prevent unauthorized changes to information system resources and provide reasonable assurance that systems are configured

and operating securely and as intended and only authorized and fully tested changes are made to critical components at each system sublevel (i.e., network, operating systems, and infrastructure applications). In addition, effectively designed and implemented configuration management controls provide reasonable assurance that applications and changes to the applications go through a formal, documented systems development process that identifies all changes to the baseline configuration. To reasonably assure that changes to applications are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be authorized, documented, tested, and independently reviewed.

In a separately issued Limited Official Use Only report, we communicated to the Board of Governors of the Federal Reserve System detailed information regarding the three new information systems general control deficiencies and made four recommendations to address these control deficiencies.

In addition, our fiscal year 2015 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, 2014, found that corrective action was complete for one of the two open recommendations and corrective action was in progress for the remaining open recommendation.

The potential effect of these new and continuing deficiencies on the Schedule of Federal Debt financial reporting for fiscal year 2015 was mitigated primarily 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. Nevertheless, these control deficiencies limit management's ability to determine whether controls are adequate to address security risks and meet the security requirements of information systems and reasonably assure that information technology products are properly configured to minimize security risks, and therefore warrant the attention and action of management.

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 is taking corrective action to address the three new information systems general control deficiencies. The Director further commented that FRB management has since addressed the remaining open recommendation from our prior year's report. We plan to follow up to determine the status of corrective actions taken on these matters during our audit of the fiscal year 2016 Schedule of Federal Debt.

- - - - -

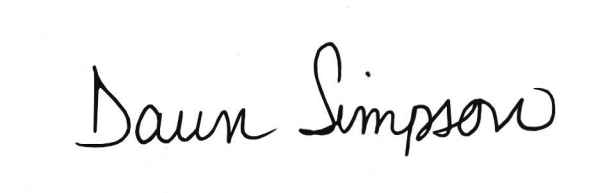
In the separately issued Limited Official Use Only report, we requested a written statement on actions taken to address our recommendations not later than 60 days after the date of that report.

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 simpsondb@gao.gov. GAO staff members who made major contributions to this report include Nicole M. Burkart, David B. Hayes, and Jeffrey L. Knott (assistant directors); Ed Brown; Dean Carpenter; and Ivy Wu.

Sincerely yours,



Dawn B. Simpson
Acting Director
Financial Management and Assurance

(100461)