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

Accessible Version

April 5, 2018

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 System 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, 2017, and 2016.[2] As part of these audits, we performed a review of information system controls over key financial systems maintained and operated by the Federal Reserve Banks (FRB) on behalf of the Department of the Treasury (Treasury) that are 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, 2017, and 2016, although certain internal controls could be improved, Fiscal Service maintained, in all material respects, effective internal control over financial reporting relevant to the Schedule of Federal Debt as of September 30, 2017, 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. However, we identified a significant deficiency in Fiscal Service's internal control over financial reporting, which although not a material weakness, is important enough to merit the attention of those charged with governance of Fiscal Service.[3] Specifically, during our fiscal year 2017 audit, we identified new deficiencies in information system controls that along with unresolved control deficiencies from prior audits collectively represent a significant deficiency in Fiscal Service's internal control over financial

[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 2017 and 2016 Schedules of Federal Debt*, GAO-18-134 (Washington, D.C.: Nov. 9, 2017).

[3]A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, 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 over financial reporting 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.

reporting. We plan to issue a separate report to the Commissioner of the Bureau of the Fiscal Service on the results of our review of information system controls over key Fiscal Service financial systems that are relevant to the Schedule of Federal Debt.

We also identified deficiencies in information system controls over key financial systems maintained and operated by FRBs on behalf of Treasury that are relevant to the Schedule of Federal Debt. However, such deficiencies in FRB information system controls did not contribute individually or collectively to the significant deficiency we identified. Nevertheless, the FRB control deficiencies warrant the attention and action of management. This report presents two new deficiencies we identified during our fiscal year 2017 testing of information system controls over key financial systems maintained and operated by FRBs on behalf of 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 system control deficiencies and associated recommendations contained in our prior years' reports that were open as of September 30, 2016. This report is a public version of a LIMITED OFFICIAL USE ONLY report that we issued concurrently.[4] The Board of Governors of the Federal Reserve System deemed much of the information in our concurrently issued report to be sensitive information, which must be protected from public disclosure. Therefore, this report omits sensitive information about the information system control deficiencies we identified. Although the information provided in this report is more limited, the report addresses the same objectives as the LIMITED OFFICIAL USE ONLY report and uses the same methodology.

Results in Brief

During our fiscal year 2017 audit, we identified two new information system general control deficiencies related to systems maintained and operated by FRBs on behalf of Treasury that are relevant to the Schedule of Federal Debt.[5] One of these deficiencies related to access controls and the other related to configuration management. In the LIMITED OFFICIAL USE ONLY report, we made two recommendations to address these control deficiencies.

In addition, during our follow-up on the status of FRBs' corrective actions to address information system control deficiencies and associated recommendations contained in our prior years' reports that were open as of September 30, 2016, we determined that corrective actions were complete for our recommendation related to access controls and that corrective actions were in progress for our remaining open recommendation related to configuration management.

These new and continuing information system control deficiencies increase the risk of unauthorized access to, modification of, or disclosure of sensitive data and programs. The potential effect of these new and continuing deficiencies on the Schedule of Federal Debt financial reporting for fiscal year 2017 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.

[4]GAO, *Management Report: Areas for Improvement in the Federal Reserve Banks' Information System Controls*, GAO-18-333RSU (Washington, D.C.: Apr. 5, 2018).

[5]General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. General controls are applied at the entity-wide, system, and business process application levels. The effectiveness of general controls is a significant factor in determining the effectiveness of business process application controls, which are applied at the business process application level.

In commenting on a draft of the separately issued LIMITED OFFICIAL USE ONLY report, the Board of Governors of the Federal Reserve System stated that the agency takes control deficiencies seriously and that FRB management is currently in the process of addressing the new and continuing information system general control deficiencies we identified during our fiscal year 2017 audit.

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 2017, FRBs issued about $8.6 trillion in federal debt securities to the public, redeemed about $8.1 trillion of debt held by the public, and processed about $248 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) maintains and operates key financial systems to process and reconcile funds disbursed and collected on behalf of Treasury.[6] FRBs process, summarize, and electronically forward data 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 federal agencies to provide information security protections for (1) information collected or maintained by or on behalf of the agency and (2) information systems[7] used or operated by the agency or by a contractor or other organization on the agency's behalf.[8] Federal law also required agencies to comply with information security standards developed by the National Institute of Standards and Technology (NIST).[9] Further, federal law required each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and

[6]National IT is an internal service provider that delivers operational and project services, enterprise information technology architecture and standards services, and enterprise information security policy and assurance services throughout the Federal Reserve System. As part of the Federal Reserve System's implementation of its System IT Strategic Plan in January 2018, National IT has been realigned to reflect a revised model for IT services. As a result, all enterprise IT infrastructure services, including those formerly branded as Federal Reserve Information Technology, are now under the direct management of the Federal Reserve System's Chief Information Officer and collectively referred to as National IT.

[7]Under federal law, an information system is defined broadly as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C. § 3502(8).

[8]During the period of our audit, federal agency information security responsibilities were provided by 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. §§ 3551–3558, which largely superseded the similar 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). In particular, the federal agency responsibilities noted in this report are codified at 44 U.S.C. § 3554.

[9]FISMA 2014, *codified at* 44 U.S.C. § 3554(a).

information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[10]

Information system general controls are the structure, policies, and procedures that apply to an entity's overall computer operations and 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.[11] An effective information system general control environment (1) provides a framework and continuous cycle of activity for managing risk, developing and implementing effective security policies, assigning responsibilities, and monitoring the adequacy of the entity's information system controls (security management); (2) limits access or detects inappropriate access to computer resources, such as data, programs, equipment, and facilities, thereby protecting them from unauthorized modification, loss, or disclosure (access controls); (3) prevents unauthorized or untested changes to critical information system resources at each system sublevel (i.e., network, operating systems, and infrastructure applications) and provides reasonable assurance that systems are securely configured and operated 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 (1) evaluate information system controls over key financial systems maintained and operated by FRBs on behalf of Treasury that are relevant to the Schedule of Federal Debt and (2) determine the status of FRBs' corrective actions to address information system control deficiencies and associated recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2016. We evaluated information system controls using the *Federal Information System Controls Audit Manual*.[12] We performed this work in connection with our audits of the Schedules of Federal Debt for the fiscal years ended September 30, 2017, and 2016, 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 system controls, we identified and reviewed FRBs' information system control policies and procedures; observed controls in operation; conducted tests of controls; and held discussions with officials at selected FRBs to determine whether controls were adequately designed, implemented, and operating effectively.

The scope of our information system general controls work for fiscal year 2017 included (1) following up on open recommendations from our prior years' reports and (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 system controls at the relevant FRBs as they relate to financial reporting relevant to the Schedule of Federal Debt.

[10]FISMA 2014, *codified at* 44 U.S.C. § 3554(b).

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

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

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 three 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.

We used an independent public accounting (IPA) firm, under contract, to assist with information system testing, including the follow-up on the status of FRBs' corrective actions during fiscal year 2017 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 findings to the Board of Governors of the Federal Reserve System, as well as to other Federal Reserve stakeholders with audit or operational responsibilities for the information system general controls and relevant application controls we tested, including representatives of FRB New York, FRB Richmond, and FRB Boston. We plan to follow up to determine the status of corrective actions taken on recommendations open as of September 30, 2017, during our audit of the fiscal year 2018 Schedule of Federal Debt.

We performed our audit in accordance with U.S. generally accepted government auditing standards. We believe that our audit provides a reasonable basis for our findings and recommendations in this report.

Assessment of FRBs' Information System General Controls

During our fiscal year 2017 audit, we identified two new information system general control deficiencies. One of these deficiencies related to access controls and the other related to configuration management.

Access controls limit access or detect inappropriate access to computer resources, such as data, programs, equipment, and facilities, thereby protecting them from unauthorized modification, loss, or disclosure. Such controls include logical access controls and physical access controls. The new access control deficiency we identified during fiscal year 2017 related to logical access controls. Effectively designed and implemented logical access controls require users to authenticate themselves through the use of passwords or other identifiers, and limit the files and other resources that authenticated users can access and the actions that they can execute based on a valid need that is determined by assigned official duties.

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 or untested changes to critical information system resources at each system sublevel (i.e., network, operating systems, and infrastructure applications) and provide reasonable assurance that systems are securely configured and operating as intended. 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 the separately issued LIMITED OFFICIAL USE ONLY report, we communicated to the Board of Governors of the Federal Reserve System detailed information regarding the two new information system general control deficiencies and made two recommendations to address these control deficiencies.

In addition, during our fiscal year 2017 follow-up on the status of FRBs' actions to address previously identified, but unresolved, information system general control deficiencies as of September 30, 2016, we found that corrective actions were complete for one open recommendation related to access controls and corrective actions were in progress for one remaining open recommendation related to configuration management.

The potential effect of these new and continuing deficiencies on the Schedule of Federal Debt financial reporting for fiscal year 2017 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 general control deficiencies increase the risk of unauthorized access to, modification of, or disclosure of sensitive data and programs and therefore warrant the attention and action of management.

Agency Comments

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 Board of Governors stated that the agency takes control deficiencies seriously and that FRB management is currently in the process of addressing the new and continuing information system general control deficiencies we identified during our fiscal year 2017 audit. We plan to follow up to determine the status of corrective actions taken to address these deficiencies and associated recommendations during our audit of the fiscal year 2018 Schedule of Federal Debt.

- - - - -

In the separately issued LIMITED OFFICIAL USE ONLY report, we requested a written statement within 60 days of the date of that report on actions taken or planned to address our recommendations.

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. 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 and Jonathan W. Ticehurst (Assistant Directors), Shaun T. Byrnes, Colleen A. Heywood, Kyusung R. Hong, Thomas J. Johnson, Werner F. Miranda-Hernandez, and Rebecca L. Perkins.
Sincerely yours,

Dawn B. Simpson
Director
Financial Management and Assurance
(102460)