Audit Report

OIG-18-013

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Federal Financing Bank's Fiscal Years 2017 and 2016 Financial Statements

November 9, 2017

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 9, 2017

**MEMORANDUM FOR THOMAS A. COLEMAN, CHIEF FINANCIAL OFFICER
FEDERAL FINANCING BANK**

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the Federal Financing Bank's Fiscal Years 2017 and 2016 Financial Statements

I am pleased to transmit the attached subject management letter. Under a contract monitored by our office, KPMG LLP (KPMG), an independent certified public accounting firm, audited the financial statements of FFB as of September 30, 2017 and 2016, and for the years then ended. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements,* as amended, and the Government Accountability Office/President's Council on Integrity and Efficiency, *Financial Audit Manual.*

As part of its audit, KPMG LLP issued the attached management letter dated November 9, 2017, that discusses a matter involving internal control over financial reporting that was identified during the audit, but was not required to be included in the auditors' reports.

In connection with the contract, we reviewed KPMG's management letter and related documentation and inquired of its representatives. KPMG is responsible for the letter and the conclusions expressed in the letter. However, our review disclosed no instances where KPMG did not comply, in all material respects, with U.S. generally accepted government auditing standards with respect to this letter.

Should you have any questions, please contact me at (202) 927-0009, or Shiela Michel, Manager, Financial Audit, at (202) 927-5407.

Attachment

This Page Intentionally Left Blank

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

November 9, 2017

Inspector General, U.S. Department of the Treasury and
the Board of Directors, Federal Financing Bank
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the Federal Financing Bank (the Bank), as of and for the year ended September 30, 2017, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and the Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirement for Federal Financial Statements*, we considered Federal Financing Bank's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Bank's internal control. Accordingly, we do not express an opinion on the effectiveness of the Bank's internal control.

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. During our audit, we noted a matter involving a deficiency in internal control. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operational efficiencies and are summarized in the attached Appendix A.

The Bank's written responses to our comments and recommendations (also in Appendix A) have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Bank's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of the addressees, Office of Manangement and Budget, the U.S Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties

Very truly yours,

KPMG LLP

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Federal Financing Bank's Loan Management and Control System (LMCS) Backups Were Not Rotated to an Offsite Location

Condition
The Loan Management and Control System (LMCS) is an internally developed application housed and maintained at Main Treasury within the Departmental Offices (DO) Data Center located in Washington, D.C., and LMCS inherits the system backup controls detailed in DO Local Area Network (LAN) System Security Plan (SSP). As such, DO performs the infrastructure-level security controls over the LMCS hardware and software on FFB's behalf, including rotating production backup's offsite.

Although the LMCS production was successfully backed up, DO did not rotate the backup media offsite on a weekly basis from August 3, 2017 through September 27, 2017 in accordance with SSP policies. Additionally, FFB management was not aware of this situation as of year-end, as DO did not disclose this issue to the FFB, and no policies or procedures exist for FY17 in which FFB monitors that the backup rotations were completed by DO.

Cause
FFB did not have a formal process to monitor DO's performance of LMCS security controls, including the rotation of backup media to the offsite location, on an ongoing basis.

Criteria
The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> SA-9 External Information System Services
>
> The organization:
>
> a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
> b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
> c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

United States Government Accountability Office Green Book dated September 2014, Section 4 *Additional Considerations,* stated:

OV4.01 Management may engage external parties to perform certain operational processes for the entity, such as accounting and payroll processing, security services, or health care claims processing. For the purpose of the Green Book, these external parties are referred to as service organizations. Management, however, retains responsibility for the performance of processes assigned to service organizations. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational process and how the service organization's internal control system impacts the entity's internal control system.

Treasury Directive Publication (TD P) 85-01, Appendix A, *Department of Treasury Information Technology Security Program,* Appendix A, "Minimum Standard Parameters, CP-9 (5), dated June 9, 2017, states:

INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE
The organization transfers information system backup information to the alternate storage site [Bureau-defined time period and transfer rate consistent with the recovery time and recovery point objectives].

DO LAN SSP dated June 29, 2017 states:
CP-(9)

If backups are stored to tape then the tape backup information shall be stored in a fireproof and waterproof locked box.

Enhancements:

(3) All DO LAN backups are stored at the alternate storage facility, First Federal.

Effect

If a disaster were to occur within the primary FFB host site, management may not be able to recover production data which could impact the integrity and reliability of the financial information.

Recommendation

We recommend that FFB management implement a process to monitor DO's performance of LMCS security controls, including the rotation of backup media to an offsite location, on an ongoing basis.

Management's Response

The FFB appreciates KPMG's and the Office of Inspector General's (OIG) review and bringing this Finding and Recommendation to our attention, and FFB management concurs with OIG's recommendation. As you outline, Treasury's Departmental Offices (DO) performs infrastructure-level security controls over the LMCS hardware and software, including the rotation of production backup tapes to an offsite location on weekly basis. Further, the FFB was unaware that from August 3, 2017 through September 27, 2017, the weekly backup tapes were not rotated offsite by DO.

The FFB has informal processes and controls, such as annual disaster recovery exercises and performing its own daily backups that are kept separate from DO's data center at FFB's 1801L St location. The FFB also performs backups during the month-end, quarter-end, and year-end processing periods. While these processes and controls test and supplement DO's backup processes, they do not include the formalized monitoring of DO's off-site tape management processes, and accordingly, did not detect the aforementioned periodic control lapse.

Accordingly, FFB management agrees to pursue and implement a process to confirm and/or monitor DO's performance of LMCS security controls, including the rotation of backup media to an off-site location. To this end, FFB management has already contacted DO to begin discussions on developing an appropriate method of control in response to this finding.

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig