Audit Report

OIG-17-027

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Office of D.C. Pensions' Fiscal Year 2016 Balance Sheet

December 16, 2016

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

December 16, 2016

MEMORANDUM FOR NANCY OSTROWSKI, DIRECTOR
OFFICE OF D.C. PENSIONS

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the Office of D.C. Pensions' Fiscal Year 2016 Balance Sheet

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 consolidated balance sheet of the Office of D.C. Pensions (ODCP) as of September 30, 2016. 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. 15-02, *Audit Requirements for Federal Financial Statements*, and the Government Accountability Office/President's Council on Integrity and Efficiency *Financial Audit Manual.*

As part of its audit, KPMG issued the attached management letter dated December 7, 2016, that discusses matters involving internal control over financial reporting that were identified during the audit. These matters relate to (1) review of STAR and Oracle audit logs and (2) removal of access of separated individuals.

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. Our review disclosed no instances where KPMG did not comply, in all material respects, with U.S. generally accepted government auditing standards.

Should you have any questions, please contact me at (202) 927-0009, or a member of your staff may contact Catherine Yi, Manager, Financial Audit, at (202) 927-5591.

Attachment

THIS PAGE INTENTIONALLY LEFT BLANK

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

December 7, 2016

Inspector General, U.S. Department of the Treasury, and
Director, Office of D.C. Pensions:

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statement of the U.S. Department of the Treasury's Office of D.C. Pensions (ODCP), which comprises the balance sheet as of September 30, 2016 and the related notes to the consolidated financial statement, in accordance with auditing standards generally accepted in the United States of America, and in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget (OMB) Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements,* we considered ODCP'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 statement, but not for the purpose of expressing an opinion on the effectiveness of ODCP's internal control. Accordingly, we do not express an opinion on the effectiveness of the ODCP'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 certain matters involving internal control and other operational matters that are presented for your consideration. 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 Appendix A to this report.

The ODCP's responses to our comments and recommendations are included in Appendix A. We did not audit the ODCP's responses and, accordingly, we express no opinion on them.

In addition, we identified certain deficiencies in internal control over financial reporting that we consider to be a significant deficiency, and communicated them in writing as Exhibit I to the Independent Auditors' Report on Internal Control Over Financial Reporting to management and those charged with governance on December 7, 2016.

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statement, 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 ODCP'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 ODCP's management, the U.S. Department of Treasury's Office of the Inspector General, OMB, 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

Washington DC

Appendix A

U.S. Department of the Treasury
Office of D.C. Pensions
FY 2016 Management Letter Comment

Lack of Review of STAR and Oracle Audit Logs

During our audit of the STAR Application and Oracle Database audit logs, we noted that the audit logs were not reviewed during Fiscal Year 2016 due to changes in roles and responsibilities for the individuals supporting the STAR Application, and the responsible personnel did not understand that it was their responsibility to perform the review. Further, we were informed that the Database administrators only review audit log files when there are issues due to the large volume of audit trail data.

The DC Pension Application Account Management for STAR, STARBASE, and supporting infrastructure subsystems procedure in Section 8.7 Monitoring, Page 12 states:

> "The application administrator will review the application server log for the previous day.
>
> The administrators will investigate unusual activity and follow the incident response policy and procedures if there is reason to believe a security incident has occurred. Unusual activity includes failed login attempts, login attempts during non-business hours, etc."

The STAR Auditing and Logs procedure, Dated June 8, 2015, Section 7 Security Monitoring, Page 9 states the following:

> Monitoring of security-related audit information shall be conducted on a regular and consistent basis:

System/Application	Task	Responsibility	Frequency
PeopleSoft	Review audit logs and monitor log size	BFS	Weekly
Oracle	Review audit logs and monitor log size	BFS	Weekly
WebLogic	Review audit logs and monitor log size	BFS	Weekly
Windows 2003	Review audit logs and monitor log size	BFS	Weekly
Solaris 10	Review audit logs and monitor log size	BFS	Weekly

According to Treasury Information Technology Security Program 85-01, Updated November 19, 2015, Appendix A, the following controls must be implemented for moderate rated systems:

AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING** Control: The organization: a. Reviews and analyzes information system audit records **[at frequency in accordance with a risk based decision and documented in the System Security Plan]** for indications of **[Bureau-defined inappropriate or unusual activity]**; and b. Reports findings to **[Bureau-defined personnel or roles].**

U.S. Department of the Treasury
Office of D.C. Pensions
FY 2016 Management Letter Comment

AU-6 (1)	**AUDIT AND ACCOUNTABILITY | Process Integration** The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
AU-6 (3)	**AUDIT AND ACCOUNTABILITY | CORRELATE AUDIT REPOSITORIES** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Without the timely review of audit logs, there is increased risk that unscrupulous, unauthorized, or inappropriate activity could be performed, which could lead to a compromise in data confidentiality, integrity, and availability.

Recommendation

We recommend that ODCP management work closely with Fiscal Service Information and Security Services (ISS) to ensure that newly assigned staff are properly briefed on the U.S. Department of Treasury policy with respect to performing and documenting reviews of audit logs.

Management's Response

"Operating system" (Windows 2003 and Solaris 10), "Infrastructure" (WebLogic), and Database (Oracle) events are being logged and reviewed by Fiscal Service. "Application" events are not considered audit logs. ODCP will work closely with Fiscal Service to identify appropriate requirements, roles and responsibilities as outlined in the STAR Auditing and Logs document, which will be updated to reflect the necessary changes.

Lack of Removal of Access of Separated Individuals

During our audit, we noted that two separated employees retained access to the STAR application after their separation date as follows:

- For one Bureau of Fiscal Service individual, although the separation and removal of access was documented, they were never removed from the system.
- For one District of Columbia Retirement Board (DCRB) individual, ODCP was not notified of the individual's separation during ODCP's weekly meeting with DCRB.

We noted that although both accounts were active 65 days after their separation dates, the accounts were not accessed during this time.

The DC Pension Application Account Management for STAR, STARBASE, and supporting infrastructure subsystems procedure in Section 2 Responsibilities, Page 4 states:

> "All user requests must be made on the "STAR Access Change Request Form" or "STAR System Access Change Request Form" or the "STARBASE Access Request Form" and approved by an authorized official.
>
> User access must be terminated for all accounts associated with a particular individual if and when that individual no longer requires access to the system. Termination of access should occur for the following situations:

- When an individual is leaving the organization
- When an individual is changing positions for which he/she no longer requires access to a specific application or system
- When a person is suspended or terminated for disciplinary/criminal reasons
- Accounts will be disabled/terminated after 90 days or less of inactivity."

According to Departmental Offices Information Technology Security Policy Handbook DO P-910, Updated April 11, 2016, Version 3.3, the following controls must be implemented:

"**3.1.2 AC-2: Account Management**

AC-2(c): System administrators shall remove all account access for DO users who have separated.

3.14.4 PS-4: Personnel Termination
General Policy: The Manager (DO employee or contractor employee) in conjunction with the System Owner (e.g., supervisor, team lead) and/or COR is responsible for:

1) Reviewing information systems/facilities access authorizations, when personnel are terminated;
2) Communicating personnel termination to facilities;
3) Removing system access for the exiting employee; and
4) Ensuring the following items are returned to DO:
   a. All Treasury documentation and media;
   b. Treasury issued computers;
   c. All other Treasury resources (Blackberries, credit cards, keys, tokens, fobs, badges, etc.)"

Without implementing effective access to programs and data controls, there is increased risk that unauthorized users could perform unscrupulous, unauthorized, or inappropriate activities, which could lead to a compromise in data confidentiality, integrity, and availability.

Recommendation

We recommend that ODCP management enforce the application account management policies and procedures to ensure timely notification and removal of individuals that no longer require access to STAR.

Management Response

ODCP will verify STAR active users with their partners/service providers on a monthly basis by reaching out to applicable parties via email requiring that they identify individuals that no longer require access to STAR. Upon notification from the partners/service providers, ODCP will follow the process outlined in the STAR Account Management Plan, which will be updated with new processes for account verification.

Treasury OIG Website

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

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx