QUALITY CONTROL REVIEW OF THE MANAGEMENT LETTER FOR THE AUDIT OF FISCAL YEARS 2016 AND 2015 FINANCIAL STATEMENTS

Department of Transportation

Report Number: QC2017025
Date Issued: February 7, 2017
Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Quality Control Review of the Management Letter for the Audit of Fiscal Years 2016 and 2015 Financial Statements, Department of Transportation Report Number: QC2017025

Date: February 7, 2017

From: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Assistant Secretary for Budget and Programs/Chief Financial Officer

I am pleased to transmit the attached management letter in connection with the audit of the Department of Transportation’s (DOT) consolidated financial statements as of and for the years ended September 30, 2016, and September 30, 2015. KPMG LLP of Washington, D.C., completed the audit under contract to the Office of Inspector General (OIG). The contract required that KPMG perform the audit in accordance with generally accepted Government auditing standards and Office of Management and Budget’s (OMB) Bulletin 15-02, “Audit Requirements for Federal Financial Statements.” KPMG issued an auditor’s report that included a clean (unmodified) opinion on DOT’s financial statements.¹

As part of its audit, KPMG issued, and is responsible for, the attached management letter that identifies internal control matters requiring management attention. KPMG was not required to include these matters or the related recommendations in its auditor’s report. The matters are as follows:

Financial Reporting and Accounting

1. Weaknesses in controls over the Federal Transit Administration’s (FTA) Grant Undelivered Orders

2. Weaknesses in Management’s Documentation of Non-Generally Accepted Accounting Principles Policies


**Information Technology General and Application Controls**

1. Weaknesses in Application Audit Log Review Controls

2. Weaknesses in Controls over Inactive Terminated Employees

3. Weaknesses in Segregation of Duties

4. Weaknesses in Periodic Review of Privileged Service Accounts

5. Weaknesses in Untimely DOT Data Center Access Review Controls

KPMG made 10 recommendations to strengthen DOT’s financial, accounting, and system controls. DOT officials concurred with KPMG’s recommendations. The Department submitted a detailed action plan to OIG dated December 23, 2016, to address the findings in KPMG’s management letter. In accordance with DOT Order 8000.1C, the corrective actions taken in response to the findings are subject to follow up.

We performed a quality control review of KPMG’s management letter and related documentation. Our review disclosed no instances in which KPMG did not comply, in all material respects, with generally accepted Government auditing standards.

We appreciate the cooperation and assistance of DOT’s representatives and KPMG. If you have any questions, please call me at (202) 366-1407, or George Banks, Program Director, at (410) 962-1729.

#

c: The Secretary
   DOT Audit Liaison, M-1

Attachment
November 30, 2016

Secretary and Inspector General
U.S. Department of Transportation

Washington, D.C.

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Transportation ("Department" or "DOT"), as of and for the year ended September 30, 2016, 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 Office of Management and Budget (OMB) Bulletin No. 15-02, Audit Requirements for Federal Financial Statements, we considered the Department'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 consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department'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 deficiencies in 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 DOT management, are intended to improve internal control or result in other operational efficiencies. The topics covered are: (A) Financial Reporting and (B) Information Technology General and Application Controls.

In addition, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies, and communicated these in writing to DOT management and those charged with governance in our report on internal control over financial report within our Independent Auditor's Report, dated November 14, 2016.

Matters specific to the Federal Aviation Administration (FAA) have been communicated to the DOT Inspector General and the FAA Administrator in a separate letter/report.

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated 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 Department 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 management and others within the Department and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP
A. Financial Reporting

Weaknesses in Controls over FTA’s Grant Undelivered Orders – DOT-2016-02

Background

The Federal Transit Administration (FTA) Grants A to Z Standard Operating Procedures Document establishes policies and procedures for FTA’s review of inactive grant projects. At the beginning of each fiscal year, by October 10th, FTA generates the Annual Grants Closeout list as of September 30 of the preceding fiscal year. The annual grants closeout list includes inactive grants that should be closed out and de-obligated during the current fiscal year, based on the following criteria:

1. A grant that is 100% disbursed;
2. A grant that was obligated more than three years ago and has not had a disbursement within the past 12 months; or,
3. A grant for operating assistance or preventative maintenance that was obligated 12 months or more ago and has not had a disbursement within the past 12 months.

The regional offices review and evaluate the status of grants included in the annual grants closeout list to determine if there are valid reasons for excluding any projects from being closed out and de-obligated during the fiscal year. All grants that are not excluded from the annual grants closeout list should be closed out and de-obligated by the end of the fiscal year.

Condition

FTA’s policy is to generate the annual grants closeout listing as of September 30 of the preceding fiscal year and therefore, the listing does not include grants that become inactive during the current fiscal year.

Recommendation

We recommend that FTA revise its policies and procedures for monitoring obligations in order to more timely identify and de-obligate stale obligations by periodically monitoring grants that become inactive during the current fiscal year.

Weaknesses in Management’s Documentation of Non-GAAP Policies – DOT-2016-03

Background/Condition

In its annual assessment of accounting policies and procedures, DOT has identified a departure from Generally Accepted Accounting Principles (GAAP) to not record an estimated liability for goods and services incurred, but not yet invoiced by the grantee or vendor. Specifically, for certain smaller Operating Administration (OA) grant programs, DOT does not record an estimated accrual for invoices not received from the grantee. In addition, for all non-grant expenses (i.e. any expense not related to a grant agreement), DOT only records an accounts payable for goods and services incurred for which an invoice has been received from the vendor, but not yet processed by DOT for payment. DOT deems an accrual for incurred but not yet billed exchange transactions to be immaterial to the DOT consolidated financial statements taken as a whole; however, management has not performed an analysis to determine the dollar impact to the DOT consolidated financial statements.

Recommendation

We recommend that DOT develop and implement guidance to formally document its assessments and recognition decisions, in accordance with Statements of Federal Financial Accounting Concepts (SFFAC) No. 5 Definitions of Element and Basic Recognition Criteria for Accrual-Basis Financial Statements, as it relates to liabilities of exchange transactions, specifically those decisions to depart from GAAP based on materiality.
Weaknesses in Controls over FTA’s Review of Manual Journal Vouchers – DOT-2016-04

Background

DOT policy is for all manual journal vouchers (JVs), recorded into the general ledger of the respective OA, to be prepared and posted by the Department’s shared services center, the Enterprise Services Center (ESC) The DOT OAs can create additional policies and procedures for their respective financial transactions.

FTA’s policy requires that an appropriate individual, from both the ESC (Division Manager) and FTA (Accountant), review and approve manual JVs prior to the entries being posted to the general ledger. The designated FTA approver will document their concurrence with the prepared journal voucher by either signing the JV coversheet or sending an email to the ESC Financial Statement group, stating their approval.

Condition

We selected a sample of 45 manual JVs from the population of FTA manual JVs for the period October 1, 2015 through September 30, 2016. Based on our review of the supporting documentation, we noted five JVs that were not reviewed timely and in accordance with FTA’s policy.

Recommendation

We recommend that FTA and ESC management revise procedures to ensure manual JVs are reviewed, by the designated FTA approver, within the timeframe established by existing policies.
B. Information Technology General and Application Controls

Weaknesses in Application Audit Log Review Controls – DOT-2016-FHWA-IT-01

**Background/Condition**

The Federal Highway Administration (FHWA) manages its federal grants in a customized grants management system, which houses the financial data. During our testing of general information technology controls, we noted that the application does not have audit log alerts in place to report/track suspicious activity nor is there a process in place for reviewing audit log activity generated by the system.

While performing our testing over the status of the remediation of these issues, we noted that there is a Plan of Action and Milestone (POAM) was created April 26, 2016 to remediate these issues; however, the remediation has not been completed.

**Recommendation**

We recommend that FHWA management:

1. Develop and implement procedures and processes that require periodic reviews of the audit logs generated by the application. In accordance with the DOT Cybersecurity Compendium requirements, the procedures should include the items being reviewed and the frequency within which the reviews should occur.
2. Update the System Security Plan to reflect the new requirements for audit log reporting and reviews.
3. Configure the system to send automated activity alerts that would notify the appropriate individuals and allow them to track suspicious activities within the system. Identify alerts that need to be generated by the system application, and develop mechanisms to generate automated alerts to notify the appropriate individuals to perform actions if an alert is generated.

Weaknesses in Controls over Inactive Terminated Employees – DOT-2016-FHWA-IT-02

**Background/Condition**

The FHWA utilizes an application to manage user access to the grants management system.

While performing our testing over general IT controls, we compared a listing of FHWA employees and contractors that had separated from the respective role during the fiscal year to an active user listing, as of April 12, 2016, to determine if the user accounts for separated employees and contractors were properly removed. We noted that one separated individual, with a termination date of February 29, 2016, improperly remained on the active user listing.

Upon notifying FHWA of the active account for a separated employee, the account was immediately deactivated on May 26, 2016.

**Recommendation**

We recommend FHWA strengthen policies and procedures to ensure that terminated users’ access is removed timely, in accordance with the DOT Cybersecurity Compendium guidelines.

Weaknesses in Segregation of Duties – DOT-2016-FHWA-IT-03

**Background/Condition**

The FHWA manages its federal grants in a customized grants management system. FHWA programmers write and submit code for system changes in Team Foundation Server (TFS), a Microsoft product that provides source code management. FHWA database administrator(s) access the code from TFS to implement changes into the production environment of the grants management system.
While performing our testing of general information technology controls, we obtained and inspected a system-generated list of programmers who have the role/responsibility to write and submit code and a system-generated list of database administrators, with access to implement code into production. Our review noted one individual that was granted both the role of programmer and the role of database administrator. Although management had a business reason for granting this dual access and processed the request through FHWA’s formal change management process, such access creates conflicting roles that should be segregated to ensure the proper internal controls over database administration.

**Recommendation**

We recommend that FHWA update policies and procedures to restrict programmer’s access from production libraries and datasets to ensure appropriate segregation of duties.

**Weaknesses in Periodic Review of Privileged Service Accounts – DOT-2016-OST-IT-01**

**Background/Condition**

FTA manages its federal grants in a customized grants management system. Server administrator access is managed by the Office of the Secretary (OST) and specifically, the DOT IT Shared Services (ITSS). ITSS is responsible for coordinating the review of privileged service accounts for continued appropriateness for all OAs in order to support their mission applications.

While performing procedures over the ITSS review of server administrator access during the FY2015 audit, we noted ITSS does not periodically initiate the review of privileged service accounts with access to in-scope FTA servers for continued appropriateness. These service accounts are user accounts that are created explicitly to provide a security context for services running on Microsoft Windows Servers and are used for server operations such as backups, vulnerability scanning, patching, and mail services.

We were informed, that on March 29, 2016, OST opened a POA&M to track the status of corrective action plans for establishing a process to initiate a semi-annual the review of all OA privileged service accounts. Consequently, during the first six months of FY2016, the first of the semi-annual reviews of privileged accounts was not performed in accordance with the semi-annual review requirement in the DOT Cybersecurity Compendium.

**Recommendation**

We recommend that OST management develop and implement privileged service account review procedures to ensure that privileged service accounts are reviewed, at least semi-annually, for continued appropriateness, based on the principle of least privileged.

**Weaknesses in Untimely DOT Data Center Access Review Controls – DOT-2016-OST-IT-02**

**Background/Condition**

During our review of the data center physical security, we were informed that access to the data center is reviewed annually. We obtained evidence of the annual data center access review, performed by the Security Operations group. We noted that on April 22, 2016, an email was sent, by the Security Operations group, to initiate the annual review. The seven team leads were instructed to verify the personnel with data center access within three business days (April 26, 2016). As of July 13, 2016, we noted that two of the seven team leads failed to respond to the request.

On July 15, 2016, we received evidence that the remaining two team leads had completed their review of personnel with data center access.
Recommendation

We recommend that the ITSS enhance data center review policy and procedures to ensure all access is reviewed for appropriateness timely, in accordance with DOT Cybersecurity Compendium guidelines.