U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

Quality Control Review of the Management Letter for the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2019 and 2018

OST

Report No. QC2020025

April 8, 2020

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

Quality Control Review of the Management Letter for the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2019 and 2018

Required by the Chief Financial Officer Act of 1990

Office of the Secretary | QC2020025 | April 8, 2020

What We Looked At

This report presents the results of our quality control review (QCR) of KPMG LLP's management letter related to the audit it conducted, under contract with us, of the Department of Transportation's (DOT) consolidated financial statements for fiscal years 2019 and 2018. In addition to its audit report on DOT's financial statements, KPMG issued a management letter that discusses eight internal control matters that it was not required to include in its audit report.

What We Found

Our QCR of KPMG's management letter disclosed no instances in which KPMG did not comply, in all material respects, with generally accepted Government auditing standards.

Recommendations

KPMG made 14 recommendations in its management letter. DOT concurred with all 14 recommendations.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: April 8, 2020

Subject: INFORMATION: Quality Control Review of the Management Letter for the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2019 and 2018 | Report No. QC2020025

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

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

I am pleased to transmit the attached management letter related to the audit of the Department of Transportation's (DOT) consolidated financial statements for fiscal years 2019 and 2018. KPMG LLP, of Washington, DC, completed the audit under contract with us. The contract required that KPMG perform the audit in accordance with generally accepted Government auditing standards and the Office of Management and Budget's Bulletin 19-03, *Audit Requirements for Federal Financial Statements*. KPMG issued an auditors' report[1] that included a clean (unmodified) opinion on DOT's financial statements.

KPMG also issued, and is responsible for, a management letter, dated November 27, 2019 (see attachment), identifying eight internal control matters that require DOT management's attention. KPMG was not required to include these matters or the related recommendations in its auditors' report.

We appreciate the cooperation and assistance of DOT's representatives and KPMG. If you have any questions, please contact me at (202) 366-1407 or George Banks, Program Director, at (202) 420-1116.

Attachment

cc: The Secretary
DOT Audit Liaison, M-1

[1] See *Quality Control Review of the Independent Auditor's Report on the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2019 and 2018* (OIG Report Number QC202020011), November 18, 2019.

Our QCR

We performed a quality control review (QCR) 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.

Summary of KPMG's Management Letter

In its management letter, KPMG reported the following matters involving DOT's internal control that require management's attention.

Weakness in the Federal Transit Administration's Grant Accrual Retrospective Review

The Federal Transit Administration's (FTA) management completed the fiscal year 2018 FTA grant accrual retrospective review by using the most recent Federal financial reports (FFR) submitted by grantees. The retrospective review is used to assess the reasonableness of FTA's grant accuracy. However, FTA's FFR information covered only 47 percent of grantees. Consequently, the information—significantly less than the historical submission rate—did not include certain FFR balances for the accrual calculation, and therefore the initial retrospective review's grant accrual amount ($1.36 billion) was $420 million or 23 percent lower than the financial statement accrual of $1.78 billion. This variance exceeded FTA's acceptable range of 10 percent.

Weakness in the Federal Railroad Administration's Monitoring of a Service Organization Report

The Federal Railroad Administration (FRA) manages grant agreements using Grant Solutions, an IT system owned by the Grants Center of Excellence, a Federal shared services center operated by the Department of Health and Human Services. As a customer of the Center, FRA should review the service organization controls (SOC-1) report to ensure the suitability of the service provider and assess its impact on FRA's grant management procedures. For example, FRA should determine if the SOC-1 contains any material impacts to its grant management

procedures. In addition, FRA should have its own complementary controls to validate the conclusions of the SOC-1 report.

During fiscal year 2019, FRA management did not demonstrate full consideration of the SOC-1 report on Grant Solutions. Specifically, KPMG noted that FRA management did not have adequate controls in place for its review of the SOC-1 report, and did not consider the updates and possible impact of the findings in the SOC-1 report on its grants management process. FRA also did not have controls to ensure the implementation and operating effectiveness of complementary user entity controls.

Weakness in the Federal Highway Administration's Periodic Review of Access for the Grants Management Application

The Federal Highway Administration's (FHWA) Office of the Chief Financial Officer (OCFO) requires divisions to review user access rights to ensure that employee access to the grants management application remains appropriate. Upon completion of the review, division offices are required to confirm to OCFO that changes to user access were not required or that changes were required and that appropriate action was taken. KPMG noted that for the month of April 2019, one division office did not complete the confirmation of its user access review.

Weakness in FHWA's Removal of Terminated Accounts for the Grants Management Application

Removal of terminated users' accounts from FHWA's grants management system was not always timely. Specifically, two employees terminated in April 2019 and one terminated in May 2019 retained access after their respective termination dates. The employees' access was removed in May and June 2019.

Weakness in FHWA's Segregation of Duties for the Grants Management Application

An instance of improper segregation of duties was identified in the grants management application. Specifically, KPMG noted that one user retained access rights to both the developer and database administrator roles.

Weakness in FHWA's User Profile and Access Control System Monthly Application Audit Log Review

FHWA's User Profile and Access Control System (UPACS) creates audit log entries to record activities such as user approval and removal; ID transfers; de-activated and re-activated IDs; failed login attempts; locked and reset passwords and PINs; user profile changes; and after-hour activities. KPMG noted that management did not maintain the reports/logs or documentation evidencing that the logs were reviewed, as mandated by the UPACS standard operating procedures (SOP).

Weakness in FHWA's Grants Management Application/UPACS Operating System Audit Logs

FHWA uses the ArcSight log management solution to review the Windows logs. FHWA management was unable to provide documented evidence of review for one of the Windows audit logs selected.

Weakness in FHWA's Grants Management Application/UPACS Database Audit Logs

FHWA uses the ArcSight log management solution to review UNIX and database logs. KPMG noted that of the five daily audit logs selected for the UNIX operating system and database, management provided one database audit log review and four operating system audit log reviews that were dated prior to log generation dates. KPMG also noted that the UNIX files were not digitally certified as the Manage and Review Log Files guidance calls for.

Recommendations

To strengthen DOT's financial, accounting, and system controls, KPMG recommended that:

1. FTA management design and implement a process to ensure that a complete population of received FFRs are considered in the retrospective review.

2. FTA management document the revised FFR submission policy in their grant methodology to consider the potential impact on the retrospective review process.

3. FRA management implement policies and procedures to establish a formal process to assess applicable third-party service organization reports that includes reviewing the SOC-1 report, reviewing and comparing reporting updates year-over-year, and reviewing findings and their impact on the grants management system.

4. FRA management implement policies and procedures to establish a formal process to assess applicable third-party service organization reports that includes implementing the service provider's recommended complementary user entity controls and monitoring these controls for proper implementation and operating effectiveness.

5. FHWA management develop and implement a process to notify appropriate authoritative personnel in the event that the division sponsor has not completed its user reviews timely ensuring that monthly reviews of user access within the application are completed by all divisions in accordance with the Fiscal Management Information System SOP.

6. FHWA management revise its current biweekly review process in coordination with Human Resources to ensure that the grants management application system owners remove terminated users within a defined time period of their termination date and that the User Access Removal SOP be updated to reflect the Human Resource coordination and the defined time period.

7. FHWA management determine the appropriate role for the grant management application user based on job function, and revoke user access to the incompatible role.

8. FHWA management ensure that access policies and procedures regarding segregation of duties are enforced when granting users access to the

grants management application via Role Based Access Control procedures as defined in the Manage Accounts SOP.

9. FHWA management develop and implement a periodic review of access for the Database Administrators and Developers for the grants management application.

10. FHWA management update the SOP, to clearly define the UPACS audit log environment, log mechanisms, and frequency and documentation of the log reviews.

11. FHWA management enforce the Manage Log Review Files SOP or similar procedure that requires the Windows System Administrator to review Grant Management Application/UPACS operating system logs on a daily basis and digitally certify the reviews on a weekly basis.

12. FHWA management ensure that System Administrators (SA) or Database Administrators (DBA) review past Grant Management Application/UPACS operating system log records for completion. If SAs or DBAs determine that the Windows Weekly log records, are not completed as required, SAs and DBAs should follow-up with the Windows System Administrator to ensure that incomplete reviews are remediated and future weekly log reviews are completed timely.

13. FHWA management enforce the Manage Log Review Files SOP or similar procedure that requires the System Administrators to review Grant Management Application/UPACS logs on a daily basis and digitally certify the reviews on a weekly basis.

14. FHWA management ensure that System Administrators (SA) or Database Administrators (DBA) review past Grant Management Application/UPACS log records for completion. If SAs or DBAs determine that the UNIX/Oracle log records, are not completed as required, SAs and DBAs should follow-up with the UNIX/Oracle System Administrators to ensure that incomplete reviews are remediated and future weekly log reviews are completed timely.

DOT officials concurred with KPMG's 14 recommendations and provided a detailed action plan to address the findings in the management letter. In accordance with DOT Order 8000.1C, the corrective actions taken in response to the findings are subject to follow up.

Exhibit. List of Acronyms

DOT	U.S. Department of Transportation
DBA	database administrator
FFR	Federal financial report
FHWA	Federal Highway Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
QCR	quality control review
SA	system administrator
SOC	service organization controls
SOP	standard operating procedure
UPACS	User Profile and Access Control System

Attachment.

Independent Auditors' Management Letter

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

November 27, 2019

Secretary, U.S. Department of Transportation
Inspector General, U.S. Department of Transportation

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the U.S. Department of Transportation (DOT) as of and for the year ended September 30, 2019, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and OMB Bulletin 19-03, *Audit Requirements for Federal Financial Statements,* we considered DOT'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 DOT's internal control. Accordingly, we do not express an opinion on the effectiveness of DOT's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our report dated November 13, 2019 on our consideration of the DOT's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be significant deficiencies.

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. In addition to the significant deficiencies noted above, we identified the following other deficiencies in internal control related to financial reporting and information technology general and application controls that are presented in Exhibit I for your consideration.

Matters specific to our separate audit of the Federal Aviation Administration (FAA) have been communicated to the Inspector General and the FAA Administrator in a separate letter.

This purpose of this letter is solely to describe the deficiencies in internal control identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Financial Reporting

Federal Transit Administration (FTA) Grant Accrual Retrospective Review (NFR-DOT-2019-01)

Background/Condition

The FTA provides grants to states, local municipalities, and other entities for public transportation projects. On a monthly basis, FTA records a grant accrual for expenses incurred by the grantees but not yet requested for payment from FTA. The grant accrual is calculated using the following formula: Grant Accrual = 1 year of disbursements x (number of days in the billing cycle) / 365.

FTA management validates the reasonableness of the grant accrual estimation methodology by performing a retrospective review over the grant accrual for the periods ending June 30, and September 30. The retrospective review calculates an individual accrual for each grant by subtracting the Federal share of expenditures reported by the grantee on each grant project's Federal Financial Report (FFR) less cumulative disbursements for the project. The total of the calculated individual grant accruals for each project are then compared to the estimated financial statement grant accrual for the related reporting period. FTA management investigates variances over 10% and, if necessary, adjusts future accrual inputs and assumptions in their methodology.

FTA Management completed the Fiscal Year (FY) 2018 FTA grant accrual retrospective review by using the most recent FFRs submitted by the grantees. However, the FFR information included in the review was incomplete and equated to only 47% of all grantees, significantly less than the historical submission rate. This resulted in a lower FFR grant accrual amount, and consequently a variance outside of the FTA acceptable range of 10%, because certain FFR balances were excluded from the accrual calculation. The FY 2018 accrual amount recorded in the financial statements was $1.78B and the initial retrospective review accrual amount was $1.36B, representing a $420M (23%) variance. FTA management subsequently reperformed the retrospective review considering all FFRs received in the 4th quarter, which resulted in a variance within the acceptable range.

Recommendation

We recommend that FTA management design and implement a process to ensure that a complete population of received FFRs are considered in the retrospective review. Further, we recommend management document the revised FFR submission policy in their grant methodology to consider the potential impact on the retrospective review process.

Federal Railroad Administration (FRA) Monitoring of Service Organization Report (NFR-DOT-2019-02)

Background/Condition

The FRA manages grant agreements using Grant Solutions, an IT system owned by the Grants Center of Excellence (GCE), which operates as part of the Department of Health and Human Services (HHS). As a customer of Grant Solutions, FRA is a named user of the HHS' System and Organization Controls (SOC-1) report, which details the examination results related to the suitability of the design and operating effectiveness of controls relevant to user entities' internal control over financial reporting. This report details any findings identified by the external auditor. As a user of an HHS system, FRA should have Complementary User Entity Controls (CUEC) in place and operating effectively to validate the conclusions of the SOC-1 report. Findings related to this system could impact FRA's ability to rely on the integrity of the system. Furthermore, FRA should properly inspect the report to ensure there are no material impacts to its Grants Management procedures. Although Grant Solutions does not interface with Delphi, FRA's grant agreements are drafted and signed in

Grant Solutions. As such, FRA should perform a proper and thorough review of the SOC-1 report to ensure the suitability of Grant Solutions as a service organization.

During FY 2019, FRA management did not demonstrate full consideration of the service organization report over HHS' Grant Solutions as follows:

- FRA management does not have a documented process or established set of procedures for the review of the SOC -1 report.
- FRA management did not consider updates to the service organization reports and the potential impacts of findings in the SOC-1 report on its grants management process during FY 2019.
- FRA does not have a documented process or established set of procedures related to ensuring the implementation and operating effectiveness of CUECs.

Recommendation

We recommend that FRA management implement policies and procedures to establish a formal process to assess applicable third-party service organization reports that includes:

- Reviewing the SOC-1 report, reviewing and comparing reporting updates year-over-year, and reviewing findings and their impact on the grants management system; and
- Implementing the service provider's recommended CUECs and monitoring these controls for proper implementation and operating effectiveness.

Information Technology (IT) General and Application Controls

Federal Highway Administration (FHWA) Periodic Review of Access for the Grants Management Application (NFR-DOT-2019-FHWA-IT-01)

Background/Condition

The FHWA utilizes a federal grant management IT application. Users of this application include state highway agencies, FHWA Division offices, and FHWA Office of the Chief Financial Officer (OCFO). OCFO requires division offices to review user access rights within their division to ensure that access remains appropriate. Upon completion of the review, division offices are required to email the FHWA OCFO and confirm that changes to user access were not required or indicate that changes were required and that the appropriate action was taken.

For the month of April 2019, one division did not complete the confirmation of its user access review.

Recommendation

We recommend that FHWA develop and implement a process to notify appropriate authoritative personnel in the event that the division sponsor has not completed its user reviews timely ensuring that monthly reviews of user access within the application are completed by all divisions in accordance with the Fiscal Management Information System SOP.

FHWA Removal of Terminated Accounts for the Grants Management Application (NFR-DOT-2019-FHWA-IT-02)

Background/Condition

The FHWA utilizes the User Profile and Access Control System (UPACS) to manage user access for its grants management application. Program managers are responsible for disabling access to applications for terminated users.

Terminated users' accounts are not always timely and appropriately removed from the FHWA grants management system. Two employees who were terminated in April 2019, and one employee who was terminated in May 2019 retained access after their respective termination dates. The employees' access was ultimately removed in May and June 2019, respectively.

Recommendation

We recommend that FHWA Management revise its current bi-weekly review process in coordination with Human Resources to ensure that the system owners remove terminated users within a defined time period of their termination date and that the User Access Removal SOP be updated to reflect the Human Resource coordination and the defined time period.

FHWA Segregation of Duties for the Grants Management Application (NFR-DOT-2019-FHWA-IT-03)

Background/Condition

FHWA is in the process of transitioning to the cloud via the Information Technology Shared Services (ITSS) consolidation effort.

Proper segregation of duties does not always exist within the grants management application for Developers and Database Administrators. Specifically, one user retained access rights to both the Developer and Database administrator roles.

Recommendations

We recommend that the FHWA:

1. Determine the appropriate role for the user based on job function, and revoke user access to the incompatible role.
2. Ensure that access policies and procedures regarding segregation of duties are enforced when granting users access to the application via Role Based Access Control procedures as defined in the Manage Accounts SOP.
3. Develop and implement a periodic review of access for the Database Administrators and Developers for the grants management application.

FHWA UPACs Monthly Application Audit Log Review (NFR-DOT-2019-FHWA-IT-04)

Background/Condition

UPACS creates log entries for various types of activities including the user approval and removal, ID transfers, de-activated and re-activated IDs, failed login attempts, locked passwords/PINs, reset passwords/PINs, user profile changes, and after-hour activities. However, management does not maintain the reports/logs or documentation evidencing that the logs were reviewed, as mandated by the UPACS SOP.

Recommendation

We recommend FHWA management update the SOP to clearly define the UPACS audit log environment, log mechanisms, and frequency and documentation of the log reviews.

FHWA Grants Management Application/UPACs Operating System Audit Logs (NFR-DOT-2019-FHWA-IT-05)

Background/Condition

The FHWA utilizes ArcSight log management solution to review the Windows logs. Management was unable to provide documented evidence of review for one of the Windows audit logs selected. (May 17, 2019).

Recommendation

We recommend ITSS enforce the Manage Log Review Files SOP or similar procedure that requires the Windows System Administrator to review logs on a daily basis and digitally certify the reviews on a weekly basis. In addition, ITSS should ensure that System Administrators (SA) or Database Administrators (DBA) review past log records for completion. If SAs or DBAs determine that the Windows Weekly log records are not completed as required, SAs and DBAs should follow-up with the Windows System Administrator to ensure that incomplete reviews are remediated and future weekly log reviews are completed timely.

FHWA Grants Management Application/UPACs Database Audit Logs (NFR-DOT-2019-FHWA-IT-06)

Background/Condition

The FHWA utilizes ArcSight log management solution to review the UNIX and Database logs. The daily logs are available for review on the ArcSight dashboard for the designated System or Database Administrator. In addition, the administrator will review the “ArcSight Suspicious Activity Review Structure” table to determine which activities require further investigation. The administrator will document the review, maintain a log recording and post the digitally signed record on a weekly basis to the ISG Procedure-Output Archive (SharePoint).

Of the five daily audit logs selected for the UNIX (operating system) and Database, management provided one database audit log review and four OS audit log reviews that were dated prior to log generation dates, resulting in documented review dates that did not reflect the week that the logs were actually generated. In addition, the UNIX files were not digitally certified, as required by the Manage and Review Log Files guidance.

Recommendation

We recommend ITSS enforce the Manage Log Review Files SOP or similar procedure that requires the System Administrators to review logs on a daily basis and digitally certify the reviews on a weekly basis. In addition, ITSS should ensure that System Administrators (SA) or Database Administrators (DBA) review past log records for completion. If SAs or DBAs determine that the UNIX/Oracle log records are not completed as required, SAs and DBAs should follow-up with the UNIX/Oracle system admins to ensure that incomplete reviews are remediated and future weekly log reviews are completed timely.

U.S. DOT OIG Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

https://www.oig.dot.gov/hotline

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590

www.oig.dot.gov