Audit Report

OIG-23-009

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2022 and 2021

December 6, 2022

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 6, 2022

MEMORANDUM FOR ANNA CANFIELD ROTH
ACTING ASSISTANT SECRETARY FOR MANAGEMENT

FROM: Ade Bankole /s/
Director, Financial Statement Audits

SUBJECT: Management Letter for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2022 and 2021

We hereby transmit the attached subject management letter. Under a contract monitored by our office, KPMG LLP (KPMG), a certified independent public accounting firm, audited the consolidated financial statements of the Department of the Treasury as of September 30, 2022 and 2021, 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 Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*, and the Government Accountability Office/Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*.

As part of its audit, KPMG issued the attached management letter dated November 15, 2022, that discusses certain deficiencies in information technology controls and financial reporting controls that were identified during the audit, but were not required to be included in the auditors' report. Management has included its response to the recommendations. These responses are unaudited. Management did not include corrective action dates in their responses, therefore these dates should be included in the Joint Audit Management Enterprise System (JAMES).

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 management letter.

If you wish to discuss this report, please contact me at (202) 927-5329, or a member of your staff may contact Shiela Michel, Manager, Financial Statement Audits, at (202) 927-5407.

Attachment

This Page Intentionally Left Blank

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

November 15, 2022

Mr. Richard K. Delmar
Deputy Inspector General
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Ms. Anna Canfield Roth
Acting Assistant Secretary for Management
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

In planning and performing our audit of the consolidated financial statements of the Department of the Treasury (the "Department") as of and for the year ended September 30, 2022, 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, 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.

We did not audit the financial statements of the Internal Revenue Service and the Office of Financial Stability, component entities of the Department. Those statements were audited by other auditors.

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 15, 2022 on our consideration of the Department's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be material weaknesses or 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. During our audit, we identified the following deficiencies in internal control which are described in Appendix A. Appendix B presents the status of the prior year comments.

The Department's responses to the findings identified in our audit are described in Appendix A. The Department's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

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

THE DEPARTMENT OF THE TREASURY

Management Letter comments

1) Segregation of Duties for Database Audit Log Reviews

Departmental Offices (DO) management has designed and implemented a control for reviewing Financial Analysis and Reporting System (FARS) database audit activity logs. However, access was not restricted to modify the database audit log configuration (i.e., the ability to modify the events that are logged) to an individual who is separate from the user activity that is logged. This conflicts with DO Information Technology (IT) Security Policy Handbook (DO-910), Version 10, which states "Audit logs must be reviewed by the ISSO or other authorized individuals who are not regular users or who do not administer access to the system." Specifically, the FARS database administrator (DBA), whose database activity is logged, has access to modify the database audit log configuration, which is a violation of the principle of segregation of duties. When identifying which systems personnel should have access to the audit related privileges, FARS management did not consider the segregation of duties risk associated with individuals who have access to modify the database audit log configuration and those whose database activity is logged.

As a result, the risk of override to circumvent the audit log control increases, ultimately increasing the risk that the audit log configuration is inappropriately modified. This increases the likelihood that unauthorized or otherwise inappropriate database user activity is not detected, investigated, and resolved in a timely manner. In addition, such activity could impact the functionality of the application and/or the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that DO management:

1. Define database access between audit-related privileges (i.e., the ability to modify the events that are logged) and other privileges.

2. Restrict access to audit-related privileges to an individual who is separate from the user activity that is logged, in accordance with segregation of duties principles.

Management Response

Management concurs with the audit recommendation to strengthen the controls related to our database layer audit logging configuration. While the FARS management team currently incorporates segregation of duties in the review of database log activity to ensure the integrity of the database layer through the secondary review conducted by the FARS technical team lead role, who is separate from the user activity being logged, documentations and safeguards can be improved to limit database administrator (DBA) role privileges related to modifying the database audit configurations to underscore the reliability of such reviews. However, our ability to implement the second recommendation—to involve a separate user other than the FARS technical team lead and DBA—is limited by resource availability, and therefore management may explore another means to address the finding. For example, our approach will seek to augment restrictions related to the DBA's ability to modify audit log configurations. Limiting the DBA's ability to modify audit log configurations would satisfy the segregation of duties issue and provide integrity to the audit log reviews conducted by the DBA and by the FARS technical team lead.

2) Periodic Review of User Access

DO Information Technology Security Policy Handbook (DO-910), Version 10.1, states: “System owners shall: Review accounts for compliance with account management requirements of users annually (privileged users semi-annually)”. And that “The information system should automatically disable any system administrator accounts that have been inactive for more than 90 days. If this is not possible, system owner shall ensure that a manual process is in place to disable inactive system administrator accounts on at least a quarterly basis.”

DO management has designed and implemented a control for recertifying privileged FARS operating system and database users’ access on a semi-annual basis. However, the operating system and database user listings used in the performance of the recertification were not system-generated and, we found that they were not a complete and accurate representation of the FARS operating system and database users and their assigned access.

There is no requirement defined in DO procedures for using system-generated user listings to perform the semi-annual recertification of privileged FARS user access. Furthermore, Departmental Offices Information Technology (DO IT) management, who is responsible for broader operating system access on the DO IT network, has not established a process for generating complete lists of FARS operating system users to support the FARS operating system and database user access recertifications.

As a result, the recertification of the database and operating user’s access was not effectively performed. This increases the likelihood that unauthorized privileged access to the operating system and/or database exists and goes undetected. Such access could be utilized to perform inappropriate activity that could alter the functionality of the application environment and/or the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that DO management update the design and implementation of their recertification of privileged FARS user access to use system-generated user listings from the FARS operating systems and database as follows:

1. Update procedures for the control implementation to include the use of system-generated lists.

2. Ensure the system-generated listings query a complete list of users and at a minimum, include attributes such as userID, name, creation date, last logon date, and assigned level of access for each user.

3. Document and retain evidence of the following:

    a. Screenshots of the query and filters/parameters/criteria used to generate FARS application, operating system, and database user access listings that are used for the recertification.

    b. The results of the recertification for each individuals/accounts access.

    c. Modification or removal of accounts where access was not recertified.

Management Response

Management concurs with the audit recommendation to update procedures and maintain documentation using system-generated lists or scripts for periodically reviewing accounts provisioned at the OS layer by DO IT, of which some accounts may retain privileged access to the FARS servers. Management will seek to improve the procedures and documentation related to the quarterly privileged access reviews performed by DO IT to address the issues identified by the audit team. We note that the OS account for the separated user in this finding is now disabled.

Separately, while the FARS management team conducts a semi-annual review, that review is limited in its scope to monitor application-layer accounts (and specific accounts we expect to see related to our technical support). The FARS management team relies on DO IT's review of OS level accounts.

3) Inadequate Review over Treasury Information Executive Repository (TIER) Fund Symbol Reference Report

The Department of the Treasury Standard Operating Procedure (SOP): FY 2022 TIER Fund Symbol Review requires an individual to "Compare corresponding values of an attribute from the TIER Fund Symbol Report and the identified External Validating Report/File [FAST Book or most recent supplemental authority] by pulling values from both sources and comparing corresponding values side by side in a worksheet" and then to "Flag Items that have discrepancies or require a more intensive review…" Additionally, it requires a second individual who "performs a more intensive review of the unresolved flags, by comparing the flagged values directly in the TIER Fund Symbol Reference Report and the validating source file/report…"

DO management did not properly review the TIER Fund Symbol Reference Report to identify an inappropriately named TIER Fund recorded in TIER and Oracle. As a result, a Treasury Account Symbol, (TAS) was given an incorrect fund name.

Management issued Standard Operating Procedure (SOP) "FY 2022 TIER Fund Symbol Review" but did not properly follow listed review procedures that would correct a misidentified TIER fund symbol attribute. As a result, DO has not performed a complete review of the entire report.

Without proper review over the new TIER fund symbol, DO management is at risk of inaccurately classifying new TIER fund symbols, recording transactions to inappropriate accounts, and therefore inaccurate financial reporting.

Recommendation

To assist management in mitigating the risk of potential inaccurate reporting and noncompliance with public laws, we recommend that management enforce full review of all TIER fund symbol following the SOP and update procedures to adequately document the review of new TIER fund symbol.

Management Response

Management concurs with the finding and will update the SOP to include the review of the "Fund Name" and fully enforce and document the review of all TIER fund symbols in accordance with these procedures. However, management notes that a Fund Name in TIER that is different from the Fast Book name does not materially increase the risk of misappropriation of budgetary resources or inaccurate financial reporting.

4) Inadequate Documentation and Untimely Review of the State and Local Fiscal Recovery Program (SLFRF) Recipients Reporting Submission

The Government Accountability Office’s *Standards for Internal Control in the Federal Government* states:

“Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system…

...Accurate and timely recording of transactions

Transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary records. In addition, management designs control activities so that all transactions are completely and accurately recorded.

*...Appropriate documentation of transactions and internal contro*l

Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.”

The Office of the Recovery Programs (ORP) management did not perform a timely review over the SLFRF monitoring of recipients reporting requirement and did not maintain sufficient appropriate documentation to support management’s review and approval of SLFRF recipient’s report data validation for use in financial reporting advance calculations. Specifically, as part of our control test work over ORP management’s review over SLFRF recipients reporting, ORP SLFRF Recipient Monitoring group was unable to timely perform its review over cumulative obligations and cumulative expenditures of the Projects and Expenditures (P&E) report as of June 30, 2022 (or P&E report as of April 30, 2022, for certain recipients) to support ORP data validation.

Although ORP management established processes and compliance testing procedures in August 2022 to monitor and review submissions from each of the SLFRF recipients including automated and manual verification checks of recipient entered data, it was not able to align the timeline of these monitoring processes with financial statement reporting.

Untimely review by the Recipient Monitoring group and inadequate documentation by the Data and Reporting team over the review of SLFRF recipients’ P&E reporting data validation increase the risk that Treasury’s total current fiscal year SLFRF expenditures may be incomplete and inaccurate, which could result in misstatements within gross costs, advances and prepayments, and disclosures.

<u>Recommendation</u>

We recommend that ORP management:

1. Continue to develop its monitoring process over review of SLFRF periodic P&E report submissions in a timely manner to support data validation of the report.

2. Develop a timeline for SLFRF monitoring and compliance testing which specifies milestones and due dates for each quarterly submission.

3. Enhance policies and procedures to include maintaining documentation to support the evidence of timely review of SLFRF recipients' periodic P&E report submission for purposes of calculating advances updates.

4. Determine the recipient monitoring resources needed to perform a timely review of the P&E report submission to align with financial statement reporting deadlines.

Management Response

Management concurs with the finding and will evaluate our existing P&E review processes, incorporate monitoring and compliance testing timelines, and enhance the documentation of management review and approval for updates to financial statement reporting.

5) Inadequate Review of ORP Manual Journal Entries

The Government Accountability Office's *Standards for Internal Control in the Federal Government* states:

"Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes performed by service organizations. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned process. Monitoring activities related to service organizations may include the use of work performed by external parties, such as service auditors, and reviewed by management."

In addition, the "*The Report on the Bureau of the Fiscal Service's Description of its Administrative Resource Center Shared Service System and the Suitability of the Design and Operating Effectiveness of its Controls – Complementary Customer Agency Controls"* states:

"…each customer agency must evaluate its own internal control to determine whether the identified Complementary Customer Agency Controls (CCACs) have been implemented and are operating effectively."

The ORP management did not have controls in place for the entire fiscal year to perform a timely review over manual journal entries prepared and posted by Treasury's Bureau of the Fiscal Service Administrative Resource Center (ARC) to validate that such journal entries were posted accurately.

ORP relies on ARC to prepare, approve and post manual journal entries related to Recovery Program transactions. ARC has a process in place to ensure proper segregation of duties between preparer and reviewer of journal entries as well as management's review and approval process before entries are recorded into the general ledger.

However, ORP did not consider the relevant CCACs for relying on ARC as a service organization to prepare and review journal entries on ORP's behalf. Although ORP started reviewing certain journal entries prepared by ARC in July 2022, it did not consistently review and approve manual journal entries throughout the fiscal year.

Inadequate controls over the review and approval of manual journal entries increases the risk that inaccurate or fraudulent transactions are posted in the general ledger.

Recommendation

We recommend that ORP management:

1. Design and implement policies and procedures that require certain manual journal entries are reviewed by ORP management prior to ARC posting the journal entry or that journal entries posted by ARC are reviewed by ORP management on a timely basis.

2. Annually, identify and ensure that the relevant complementary customer agency controls listed in The Report on the Bureau of the Fiscal Service's Description of its Administrative Resource Center Shared Service System and the Suitability of the Design and Operating Effectiveness of its Controls are considered in the design and implementation of controls at ORP.

Management Response

Management concurs with the finding and will enhance policies and procedures to ensure adequate controls over the review and approval of manual journal entries.

Appendix B

THE DEPARTMENT OF THE TREASURY

Status of Prior Year Management Letter Comment

Fiscal Year 2021 Management Letter Comment

1. Timely Removal of Terminated Users from FARS Needs Improvement

   Fiscal Year 2022 Status – Open

2. Vulnerability Program Management Implementation

   Fiscal Year 2022 Status – Resolved

3. DO IT Privileged User Access Review

   Fiscal Year 2022 Status – Resolved

4. FARS Audit Log Review

   Fiscal Year 2022 Status – Resolved

5. Lack of Timely Completion by Fiscal Service and Departmental Offices Monitoring of the Core Trial Balance (TB) to TIER Reconciliation

   Fiscal Year 2022 Status – Resolved

6. Inadequate Review over TIER Fund Symbol Reference Report

   Fiscal Year 2022 Status – This finding has been reissued as deficiency #3 above.

7. Ineffective Review over the FECA Liability Allocation

   Fiscal Year 2022 Status – Resolved

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/