Audit Report

OIG-24-008

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2023 and 2022

December 6, 2023

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D. C. 20220

December 6, 2023

MEMORANDUM FOR ANNA CANFIELD ROTH
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 2023 and 2022

We hereby transmit the attached subject report. 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, 2023 and 2022, 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. 24-01, *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, 2023, that discusses certain deficiencies in information technology 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) 486-1415.

Attachment

This Page Intentionally Left Blank

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

November 15, 2023

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

Ms. Anna Canfield Roth
Assistant Secretary for Management
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, 2023, 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 or the Office of Financial Stability - Trouble Asset Relief Program, 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, 2023 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.

The 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) Privileged Database Account Password Settings Weakness

Financial Analysis and Reporting System (FARS) database password authentication was not implemented in accordance with Departmental Offices Information Technology Security Policy Handbook (DO-910) and the FARS System Security Plan (SSP). Specifically, the FARS database password settings were configured to allow for five invalid login attempts before account lockout; however, DO-910 and the FARS SSP require that password settings enforce a limit of three invalid login attempts. FARS management did not prioritize the enforcement of DO-910 password authentication requirements at the FARS database layer, since users first authenticate at the network/operating system layer before they can authenticate to the database.

As a result of the noted condition, the risk of brute force attack is increased. This increases the likelihood that unauthorized or otherwise inappropriate database user access is granted. In addition, such access could impact the confidentiality, integrity, and availability of the system and its data.

As a response to the above deficiency, management implemented changes to the password configuration in early FY2024.

Recommendation

We recommend that Departmental Offices (DO) management:

1. Review DO-910 and FARS SSP password setting requirements to determine if they apply to all layers of system technologies (e.g., application, database, and operating system). If necessary, consider specifying distinct password setting requirements for the different layers.

2. Implement password authentication controls at the FARS database in accordance with the minimum requirements set by DO-910 and the FARS SSP, to include the number of failed login attempts allowed.

Management Response

DO management concurs with the audit recommendation to adjust the FARS database password settings to align with the DO Information Technology (IT) Security Policy. DO management employs robust multi-factor authentication protocols across multiple architectural layers to safeguard FARS access and is committed to enforcing DO IT Security policies. As such, management took immediate action to rectify the issue and provided auditors with evidence of configuration changes made to comply with the procedure and satisfy the audit recommendation. The auditors have acknowledged, upon review, that the corrective actions taken by FARS management to remediate this issue suffice to close this NFR effective November 2023.

2) Periodic Privileged Operating System Access Review Weakness

Office of the Chief Information Officer (OCIO) – DO IT management's control for quarterly reviewing and reauthorizing privileged FARS operating system (OS) access was not sufficiently designed and implemented. Specifically:

- Supporting documentation evidencing management's performance of the review and reauthorization, as well as the resulting determinations, was not documented and retained.
- The individual responsible for review and reauthorization reviewed his own access, and therefore is not independent with respect to his own review.
- The review does not include a review of user access to service groups/accounts.

OCIO – DO IT management's policies and procedure did not specify the proper evidence and documentation needed to support the quarterly review control, the proper segregation of duties so as to not review an individual's own access, and the expectation for the review to encompass all user access, including user access to service groups/accounts.

As a result of the noted condition, the risk is increased that inappropriate or unauthorized access could be retained at the OS layer without timely management knowledge. Such access could be used to impact the availability of the system and its data.

Recommendation

We recommend that DO management:

1. Develop policies and procedures for performing the quarterly review and reauthorization of privileged OS access, which specify:
    - How to document the review of user access for continued appropriateness and the resulting determinations.
    - Assignment of individual(s) responsible for performing the review(s) across the various privileged OS domains/groups/accounts, who are independent of the access they review and are of the appropriate authority.
    - Identification/Inventory of the privileged OS domains/groups/accounts that are subject to review, to include any privileged OS service groups/accounts.
2. Disseminate said policies and procedures to control performers and re-perform a review and reauthorization of privileged OS access that enforces independence from an individual reviewing their own access, includes OS service groups/accounts, and is documented/retained, in accordance with the established policies and procedures.

Management Response

DO management concurs with the deficiency noted above. To meet recommendation #1, DO management will follow the Treasury Shared Service Enterprise Cybersecurity Policy for SI-12 and AC-5. DO management will develop procedures to explicitly explain the DO process for reviewing, recertifying, and reauthorizing privileged users on the DO Enterprise accounts and groups. This will include an Information Systems Security Manager/Officer review of the reviews to ensure Separation of Duties is upheld.

To meet recommendation #2, DO management will email procedures, citing the policy, to designated reviewers upon initial drafting of the updated procedures, and quarterly thereafter with the reviewer's list of accounts for action.

3) Review of the ARC Budget Rollup Journal Entry

The General and Special Entity Accounting Group (GSEA) utilizes the Treasury's Bureau of the Fiscal Service Administrative Resource Center (ARC) for processing transactions for the administrative funds of the Government Sponsored Enterprises (GSE).

At the beginning of each fiscal year, ARC, on behalf of GSE, posts transactions through a budget module that reverses the prior Budget Fiscal Year (BFY) funds that are Appropriated, Apportioned, Unapportioned – Unexpired and Allotted to roll the available balance forward to current BFY funding. ARC prepares and posts a simultaneous entry to re-appropriate, reapportion, and reallot the funds into the new BFY. In combination, these transactions are referred to as the "Budget Roll Forward".

At the beginning of the Budget Roll Forward process and prior to posting the transactions above, the Budget Analyst (Analyst) prepares and completes the steps in the Carryover Review checklist. Two of the steps include (1) verifying all September activity has been posted and (2) obtaining confirmation from the Customer Care Branch (a group within ARC) that the prior fiscal year had successfully closed. The Analyst then prepares and posts the Budget Roll Forward transaction in the general ledger. Once the entry is posted, the ARC Reviewer reviews the transactions to ensure it is accurately recorded and manually approves the transaction in the Budget Upload template.

For the Budget Roll Forward process between fiscal year (FY) 2023 and FY 2024, the ARC Analyst did not prepare (and self-review) the transactions uploaded to the general ledger prior to posting GSE related transactions, nor did they obtain confirmation from the Customer Care Branch that the previous fiscal year had successfully closed.

ARC management indicated that ARC Analyst responsible for preparing the Carryover Review and posting the transactions did not complete the required steps due to an oversight and the volume of workload in their schedule.

ARC management has also indicated that the ARC Reviewer did not complete their review of the posted transactions timely due to time constraints. ARC's policy does not prescribe a timeline of review requirements for the Budget Roll Forward transactions.

Inadequate controls over the review and approval of Budget Roll Forward transactions increase the risk that inaccurate transactions are prepared and posted in the general ledger. In this instance, as of and for the period ended September 30, 2023, Fund Balance with Treasury, Unexpended Appropriations, Appropriations Realized, Unapportioned – Unexpired Authority, Apportionments, and Allotments were misstated in the general ledger by approximately $254 billion.

However, the related financial statement line items in Treasury Information Executive Repository, the U.S. Department of Treasury's financial reporting system and repository, were correctly recorded as of and for the year ended September 30, 2023.

Recommendation

We recommend that DO management work with ARC management to:

1. Provide sufficient training to ARC Analysts and validate that ARC Analysts have sufficient capacity to complete all required steps of the Carryover Review process checklist prior to preparing and posting transactions related to the Budget Roll Forward process in accordance with management's policies and procedures.

2. Include and enforce an appropriate timeline of review requirements in the policies and procedures for ARC Reviewers to perform a timely review of posted transactions related to the Budget Roll Forward process and other significant and complex transactions.

Management Response

Management concurs with the finding and recommendations. Specifically, we have already provided additional training to our budget analysts relating to the year-end carryover review process and taking steps to ensure that they complete all required steps of the Carryover Review process checklist for ensuring that the prior year period is closed before posting transactions in the financial system to complete the carryover process. Further, we are looking for opportunities to revise our secondary review procedures and timelines for the posting of transactions during the carryover process and other significant and complex transactions to ensure a more timely review and further mitigate the risk of errors in the future.

THE DEPARTMENT OF THE TREASURY

Status of Prior Year Management Letter Comment

Fiscal Year 2022 Management Letter Comment

1. Timely Removal of Terminated Users from FARS Needs Improvement

   Fiscal Year 2023 Status – Resolved

2. Segregation of Duties for Database Audit Log Reviews

   Fiscal Year 2023 Status – Management remediated the recommendations in FY2023. Due to the timing of the remediation, KPMG considers this finding partially closed and will determine if remediation has fully occurred in subsequent audit years.

3. Periodic Review of User Access

   Fiscal Year 2023 Status – Resolved

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

   Fiscal Year 2023 Status – Resolved

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

   Fiscal Year 2023 Status – Resolved

6. Inadequate Review of ORP Manual Journal Entries

   Fiscal Year 2023 Status – Resolved

This Page Intentionally Left Blank

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/