Audit Report

OIG-22-014

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2021 and 2020

December 1, 2021

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 1, 2021

MEMORANDUM FOR J. TREVOR NORRIS
ACTING ASSISTANT SECRETARY FOR MANAGEMENT

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

SUBJECT: Management Letter for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2021 and 2020

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, 2021 and 2020, 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. 21-04, *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, 2021, 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.

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 R. Nikki Holbrook, Acting Manager, Financial Statement Audits, at (202) 927-6552.

Attachment

This Page Intentionally Left Blank

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

November 15, 2021

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

Mr. J. Trevor Norris
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, 2021, 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, 2021 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

Appendix A

THE DEPARTMENT OF THE TREASURY

Management Letter comments

1) Timely Removal of Terminated Users from FARS needs Improvement

The Departmental Offices (DO) Information Technology Security Policy Handbook (DO-910) states "System administrators shall remove all account access for DO users who have separated…" In addition, the general policy for personnel termination includes disabling information system access as soon as possible, but no later than 24 hours, and also notifying appropriate personnel as soon as possible, but no later than 24 hours.

The Financial Analysis and Reporting System (FARS) management team has implemented a control for removing the access of terminated users from Treasury Information Executive Repository (TIER) and TIER Financial Statements (TFS); however, the timeframe for removing terminated user access is three business days from the receipt of notification rather than from the user's separation date, which elongates the amount of time that a user could retain unauthorized access to the system indefinitely.

As a result, we noted the following:

- one terminated user with an effective termination date of January 2, 2021 did not have access removed until April 21, 2021, one day after FARS management was notified that the user had been inactive for 120 days.
- one terminated user with an effective termination date of December 15, 2020 was not removed from TFS and TIER until March 12, 2021, two days after FARS management was notified to remove the access.

A lack of timely removal of system access of terminated employees and/or contractors increases the risk of users retaining unauthorized and/or inappropriate system access. Such access could allow an individual to advertently or inadvertently perform unauthorized activity that would impact the functionality of the application and/or the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that DO management:

1. Establish a timeframe requirement for removing or disabling system (e.g., FARS) access of terminated employees and contractors that is from the user's effective termination date. This established timeframe requirement should be included in the DO-910 policy.
2. Develop, document, and implement procedures that enforce the above timeframe for removing or disabling system (e.g., FARS) access of terminated users. This may include timely notification from DO management to system (e.g., FARS) management of user's termination dates.

Management Response

Management concurs with this finding and will coordinate as needed with Office of the Chief Information Officer (OCIO) to update the language of control PS-4 in DO 910 to reflect a time window appropriate for disabling access to the FARS upon a user's effective termination date. The FARS team will further address this finding by allowing FARS users to use only those authentication methods to log into FARS applications that would be immediately disabled by the bureau from which a terminated employee is separating, once

that bureau disables the terminated employee's network access and completes other steps in the bureau exit process. When a terminated user's network access and other permissions are revoked upon termination, these FARS authentication methods would be rendered disabled and the user would be unable to access FARS applications. This approach will achieve compliance with the DO 910 requirement in control PS-4 for "disabling information system access" for FARS users within the time window specified by DO 910.

2) Vulnerability Program Management Implementation

The Treasury Directive Publication 85-01, Appendix A, Minimum Standard Parameters for Non-National Security Information and Information System requires vulnerability scanning to be performed every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported.. However, for the months of January 2021, February 2021, and March 2021, DO management did not perform vulnerability scans for the FARS application and database layers. Management continued to meet monthly to discuss identified vulnerabilities; however, during that time, new vulnerabilities were not identified until scanning resumed in the month of April 2021.

OCIO management halted vulnerability scanning activities for the period of January 13, 2021 through April 16, 2021 to accommodate a technical assessment of the DO information technology (IT) infrastructure after a suspected security incident. This included the vulnerability scanning performed by three scanning tools used throughout the DO bureau which normally perform monthly vulnerability scans of FARS servers.

Without performing vulnerability scanning for the FARS application and database monthly, there is an increased likelihood that vulnerabilities go undetected and un-remediated in a timely manner. Such vulnerabilities could be exploited, which would compromise the confidentiality, integrity, and availability of the system and its data.

Recommendation

As DO management re-implemented FARS vulnerability scanning on April 16, 2021, we recommend that management continue to conduct monthly vulnerability scans, as required by policy, and address identified vulnerabilities in a timely manner.

Management Response

Management concurs with the finding but would point out that the OCIO decision to halt monthly vulnerability scans throughout the DO bureau was necessary to address extraordinary circumstances. Given the circumstances, the FARS security team took alternative measures to review vulnerabilities during the period in which scans were halted. The FARS security team will continue to perform monthly vulnerability scans and—as we have done for every month of fiscal year (FY) 2021, including January through March 2021—review the results and remediate vulnerabilities in a timely manner.

3) DO IT Privileged User Access Review

The Departmental Offices Information Technology Security Policy Handbook (DO-910) states system owners shall "Review accounts for compliance with account management requirements of users annually (privileged users semi-annually)." In FY2021, DO management did not review privileged DO IT users on at least a semi-annual basis as required by the policy.

DO management was aware that they were non-compliant with the DO policy requirement for performing privileged user reviews on at least a semi-annual basis and had plans to implement a quarterly privileged user review control to achieve compliance. DO management was unable to complete implementation of the quarterly review control in FY21 as they had identified staffing constraints for assigning a dedicated control performer.

Failure to periodically review privileged user access for appropriateness on a complete, accurate and timely basis increases the risk of users having unauthorized and/or inappropriate system access. Such access could allow an individual to advertently or inadvertently perform unauthorized activity that would impact the functionality of the application and/or the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that DO management implement a review of privileged DO IT users that is performed on at least a semi-annual basis as required by DO policy (DO-910).

Management Response

Management concurs with the finding and will fully implement the recommendation to review the access of privileged DO IT users on a semi-annual basis. Such a review was conducted earlier in FY 2021 by a staff member who has since separated from the DO bureau. That review of privileged DO IT users was not sufficiently documented. Subsequent semi-annual reviews of privileged DO IT users will be documented and maintained for review.

4) FARS Audit Log Review

The Departmental Offices Information Technology Security Policy Handbook (DO-910) states that information systems shall be configured to monitor minimum auditable events including account logon events, account management, directory service access, logon events, object access and others. In addition, Government Accountability Office (GAO), Standards for Internal Controls in the Federal Government, September 2014 (Greenbook) states "Responses to Objectives and Risks 10.02, "Management designs control activities in response to the entity's objectives and risks…. Management designs control activities to fulfill defined responsibilities and address identified risk responses.""

FARS management utilizes an audit log tool that captures user and system level activity for review within a reviewer dashboard; however, management has not defined and documented an audit log review process that includes defined inappropriate or unusual activity, as well as specific process steps associated with reviewing and analyzing audit logs for indications of inappropriate or unusual activity.

FARS management did not consider the need to define unusual or suspicious activity, such that an adequate review of audit logs for unusual or suspicious activity can be performed.

Without an audit log review process that includes defined unusual or suspicious activity, FARS management is unable to monitor/review all security event data and identify, evaluate and, if necessary, respond to potentially unauthorized system activities. As a result, the risk is increased that such unauthorized activities are not identified, investigated, and resolved in a timely manner, thereby impacting system, application, and data integrity.

Recommendation

We recommend that FARS management:

1. Review and update the FARS audit events that are logged and reviewed on an on-going basis and document a rationale for why the auditable events are deemed to be adequate.

2. Update existing policies and procedures to define inappropriate or unusual activity.

3. Update existing policies and procedure to facilitate how review activities for all audit events must be performed and documented, including the identification and escalation of any inappropriate or unusual activity.

4. Ensure that the audit log review tool is configured to support the investigation of unusual or suspicious activity based on defined thresholds and/or alerts.

Management Response

Management concurs with the finding, and the FARS team will follow the associated recommendations to explicitly document audit log review procedures and definitions. However, management would point out that the FARS team does maintain a template checklist document (provided to auditors) which reflects the standard audit log review procedures followed by the FARS Information System Security Officer (ISSO) each quarter. The template checklist also reflects definitions and thresholds of what constitutes unusual or suspicious activity for auditable events. This checklist, along with data from the Splunk tool, enables the FARS ISSO to conduct an adequate review and analysis of security event data within the FARS audit logs each quarter and, if necessary, respond to potentially unauthorized system activities.

KPMG Response

We have conducted our audit in accordance with auditing standards generally accepted in the United States of America.

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

The Departmental Accounting Policy OFRP-16-02 requires "The reconciliation and related TIER manual adjustment documentation, along with review and approval processes, must be completed before the upload of the final TIER data file to the TIER repository." DO delegated the responsibility to perform the Core TB to TIER reconciliation to the Department's Bureau of the Fiscal Service (Fiscal Service) Administrative Resource Center (ARC), a shared service provider. During our testing of the March 2021 reconciliation, ARC did not perform the Core TB to TIER reconciliation in a timely manner. This was evidenced by the report run dates on all of the TIER generated reports in the DO TIER Checklist for the month, as well as a follow-up inquiry by KPMG, where management indicated to us that the reconciliation was not performed and documented until September 24, 2021. Additionally, we obtained the reconciliations for the months of December 2020 – February 2021 and noted evidence of the completion of the reconciliations found on the DO TIER Checklists was not documented until July 8, 2021. Further, we also note the reconciliations for November 2020, July 2021, and August 2021 were not completed.

Management did not effectively monitor procedures performed at the ARC shared service provider to ensure monthly Core TB to TIER reconciliations were performed in a timely manner.

Without timely performance of this control, differences between the Core TB and TIER file might not be resolved before the upload of the final TIER data file. This could lead to potential misstatements in the Department's consolidated financial statements and related footnotes that are not prevented or detected and corrected on a timely basis.

Recommendation

DO management should implement monitoring policies and procedures to ensure ARC performs the Core TB to TIER reconciliation timely and in accordance with the current Departmental Accounting Policy.

Management Response

Management concurs with the finding that monitoring procedures were not effectively performed over ARC shared service provider to ensure monthly CORE TB to TIER reconciliations were performed in a timely manner. Management will implement monitoring policies and procedures to ensure ARC performs the Core TB to TIER reconciliation timely and in accordance with Treasury's current Departmental Accounting Policy.

6) Inadequate Review over TIER Fund Symbol Reference Report

The GAO Green Book states the following, “Management designs control activities in response to the entity’s objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management’s directives to achieve the entity’s objectives and address related risks.

DO did not properly review the TIER Fund Symbol Reference Report to identify an inappropriately coded TIER Fund Symbol. As a result, the Minority Lending Program, or TAS Number “020 x0160000” was coded in the “REVOLVING” Fund Group, when it should have been coded as “GENERAL.” The Minority Lending Program does not meet the criteria for a “REVOLVING” fund as defined by Office of Management and Budget (OMB) Circular A-11.

Management does not have documented Standard Operating Procedures for the review of the TIER Fund Symbol Reference Report. As a result, DO has not performed a complete review of the entire report. Without proper review over the new fund symbols, DO is at risk of inaccurately classifying new TASs, and therefore inaccurate reporting.

Recommendation

To assist management in mitigating the risk of potential inaccurate reporting and noncompliance with public laws, we recommend that management complete a full review of all TASs, compare all attributes to the Federal Account Symbols and Titles (FAST) book, and create policies and procedures to adequately document the review of new TASs.

Management Response

Management concurs with the finding that documented Standard Operating Procedures do not exist for the review of the TIER Fund Symbol Reference Report. Management will implement policies and procedures to ensure a complete and full review of all TASs, compare all attributes to the Federal Account Symbols and Titles book, and adequately document the review of new TASs.

7) Ineffective Review over the FECA Liability Allocation

As part of the Fiscal Year-End financial reporting process, DO – Financial Reporting and Policy (FRP) group is responsible for compiling the Department’s Federal Employees’ Compensation Act (FECA) liability worksheet using the Department of Labor’s (DOL) Office of Workers Compensation Programs Chargeback Agency Billing Summary, and DOL’s Estimates of Total FECA Future Liabilities as of the Fiscal Year-End. The worksheet compiled by the FRP group includes a calculation of the current year’s FECA actuarial liability, by component, using the past 5 years’ data. KPMG noted the Bureau of Engraving and Printing (BEP) recorded more than the amount allocated to BEP by the FRP group resulting in an overstatement of the FECA actuarial liability and related gross costs of $1,414,147.87 within Oracle.

BEP recorded the FECA actuarial liability and related gross costs based on the DOL data, and not the allocation calculated by the FRP group. Management did not perform an effective review of the current year FECA actuarial liability and related gross costs recorded by the components.

Without effective review over the FECA transactions recorded by the components, differences between the FECA liability worksheet and trial balance may exist. Management's ineffective review over the FECA liability led to a current year overstatement of $1,414,147.87 in the U.S. Standard General Ledger accounts 22250000 (Unfunded FECA Liability) and 68500000 (Employer Contributions to Employee Benefit Programs Not Requiring Current-Year Budget Authority (Unobligated)), and could lead to future misstatements in the consolidated financial statements and related disclosures. This has resulted in an overstatement of Other Liabilities and Gross Costs in the Department's Consolidated Balance Sheet and Statement of Net Cost, respectively.

Recommendation

DO-FRP should implement monitoring policies and procedures to ensure components are accurately recording their FECA actuarial liability and related gross costs in the General Ledger. For any differences noted, DO-FRP should investigate and resolve accordingly.

Management Response

Management concurs with the finding and will develop and implement monitoring procedures to ensure components are accurately recording their FECA actuarial liability and related gross costs in the General Ledger.

Appendix B

THE DEPARTMENT OF THE TREASURY

Status of Prior Year Management Letter Comment

Fiscal Year 2020 Management Letter Comment

1. Timely Removal of Terminated Users from FARS and DO IT Needs Improvement

   Fiscal Year 2021 Status – In FY 2020, this finding had been bifurcated in order to separate and better align the responsibilities of FARS and DO IT management. Department management remediated the underlying conditions related to the timely removal of terminated users from DO IT systems. However, the finding related to the timely removal of terminated users from FARS systems has not been remediated and re-issued with new conditions as current year finding #1.

2. Vulnerability Program Management Implementation

   Fiscal Year 2021 Status – This finding has been re-issued with new conditions as current year finding #2.

3. Frequency and Evidence of FARS Backups

   Fiscal Year 2021 Status – Remediated

4. Timeliness of Control Documentation Availability

   Fiscal Year 2021 Status – Remediated

5. Untimely Recording of the Quarterly Government-Sponsored Enterprises Liquidity Preference Increase

   Fiscal Year 2021 Status – Remediated

6. Lack of Appropriate Review of Judgment Fund Internet Claims System Year-end Accrual

   Fiscal Year 2021 Status - Remediated

7. Lack of Documentation of Review over Federal Managers' Financial Integrity Act Compliance Testing Results; and Incorrect Compilation on the Statement of Assurance Review Sheet

   Fiscal Year 2021 Status - Remediated

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/