



Audit Report



OIG-21-020

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Department of the Treasury's Financial Statements for Fiscal Years 2020 and 2019

December 30, 2020

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 30, 2020

**MEMORANDUM FOR DAVID F. EISNER
ASSISTANT SECRETARY FOR MANAGEMENT**

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the Department of the Treasury's Financial Statements for Fiscal Years 2020 and 2019

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 financial statements of the Department of the Treasury as of September 30, 2020 and 2019, 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. 19-03, *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 December 30, 2020, 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' reports.

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) 927-0009, or a member of your staff may contact Ade Bankole, Manager, Financial Audit, at (202) 927-5329.

Attachment



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

December 30, 2020

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

Mr. David F. Eisner
Assistant Secretary for Management
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 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, 2020, 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 in accordance with Office of Management and Budget (OMB) Bulletin No. 19-03, Audit Requirements for Federal Financial Statements, we considered the Department's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

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 first 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 December 30, 2020 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 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 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. Vulnerability Program Management Implementation

The Department of the Treasury's (Treasury) directive publication appendix A requires minimum standard parameters for non-national security information and information systems. Specifically, vulnerability scanning should be performed every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported. However, as part of our testing over Vulnerability Program Management, we identified for the period of October 1, 2019 through June 30, 2020, vulnerability scans were not implemented and being performed for the Financial Analysis and Reporting System (FARS) application and database layers.

FARS management had prioritized the implementation of a vulnerability management program for the FARS application and database based on previous independent auditor findings dating back to 2017. However, due to the extent of remediation effort to implement tools sufficient to address the findings, Departmental Offices (DO) management was unable to implement a solution prior to May 2020 and subsequently closed the tracking of the prior-year findings in June 2020.

Without having an implemented vulnerability scanning program/tool for the FARS application and database for approximately nine months out of the year, there is an increased likelihood that vulnerabilities could go undetected and unremediated. Such vulnerabilities could be exploited, which would compromise the confidentiality, integrity, and availability of the system and its data.

Recommendation

As FARS management fully implemented a vulnerability scanning program/tool in June 2020 and for the rest of Fiscal Year (FY) 2020, we recommend that management continue to conduct monthly vulnerability scans, as required by policy, and address identified vulnerabilities as appropriate.

Management Response

The original weakness (for a lack of both web application and database scanning) was tracked as Plan of Action and Milestones (POA&M) #16529, in accordance with TDP 85-01, CA-5, and DO-910, CA-5 policy. The POA&M process is overseen by the System Owner with support from the Information System Security Officer (ISSO). POA&M #16529 was reviewed and updated quarterly at a minimum (in accordance with TD P 85-01, CA-5_N.01) by the FARS team, including the FARS ISSO, as evidenced by the minutes of monthly FARS POA&M status meetings. The FARS team remediated the web application scan issue in January 2020 and the database scan issue in May 2020, which enabled the FARS team to mark the POA&M as completed on June 3, 2020.

While, management concurs with this finding, management would like to further clarify:

- Monthly scan results from both web application scans and database scans are available for evaluation to assess compliance with control RA-5.
- Because both database and application vulnerability scans have been performed on a monthly basis since June 2020, this finding does not drive any improvement to the process. While we understand we did not have new controls fully in place until June 2020, we would have expected the audit team to test our controls from June through September 2020, since there was ample time to assess the effectiveness of these controls.

KPMG Response

We have conducted our audit in accordance with auditing standards generally accepted in the United States of America and our report on internal controls over financial reporting encompasses the entire year under audit.

2. Frequency and Evidence of FARS Backups

Treasury's directive publication appendix A, the DO information technology (IT) security policy handbook, and the FARS system security plan require that backups for low and moderate FIPS 199 rated information systems adhere to a weekly backup schedule. However, as a result of our testing of operating effectiveness over FARS backup controls, we identified that DO IT management did not retain audit evidence to demonstrate the completion of FARS backups. Specifically, for 14 of the 15 requested dates, DO IT management was unable to provide FARS backup logs evidencing that the daily incremental backups were performed. Additionally, we identified that the frequency of full backups, which is required by DO and Treasury policy to be performed at least weekly, was changed to every-other week for the period after June 2020.

Without evidence of backup logs, DO management's ability to properly manage, monitor, and/or evaluate the backup process for ongoing effectiveness, could be inhibited. Furthermore, without performing backups at the required frequency, the likelihood of data loss due to a disaster or emergency increases. Ultimately, this could compromise the confidentiality, integrity, and availability of the system and its data.

Recommendation

We recommend that DO IT management:

1. Ensure that the configured schedule/frequency of FARS backups is implemented in accordance with the minimum backup frequency required by DO and Treasury policy.
2. Ensure that system-generated logs of backups, including failures, are retained for the examination period and can be provided upon request.

Management Response

DO IT has generally operated at Level 3 of the maturity model outlined in the Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. DO IT has implemented a program to move to Level 4 of this maturity model and will include metrics related to backup performance in the program. DO IT will also modify our backup policies to reflect backup frequency and retention driven by system- and user-based metrics.

3. Timeliness of Control Documentation Availability

According to the Government Accountability Office's standards for internal controls in the Federal Government and Office of Management and Budget circular A-123, management's responsibility for enterprise risk management and internal controls requires that management develop and maintain effective internal controls that allows for documentation to be readily available for examination. However, DO management was unable to timely provide documentation to evidence the design and implementation of controls related to DO IT account management – Access request form/evidence of approval for a new user and the annual user access review documentation concerning privileged users; DO IT vulnerability management – completed monthly vulnerability scan of DO IT, including scan results, monthly review meeting minutes, and evidence of follow-up of vulnerabilities identified; and FARS audit logging – FARS Treasury Information Executive Repository (TIER) and TIER Financial Statements system-generated 24-hour audit log activity and audit log review history file.

DO management subsequently provided the supporting documentation after audit workpapers had been provided to the Office of Inspector General for review.

The untimely availability of documentation could inhibit DO management's ability to properly manage, monitor, and/or evaluate such processes to help ensure their ongoing effectiveness. Such changes could negatively affect the completeness, accuracy, and availability of the system and its data.

Recommendation

We recommend that DO management communicate that requested documentation evidencing the design and implementation of the internal controls should be readily available for examination under remote working conditions.

Management Response

Management concurs with the finding that documentation was not furnished in a timely manner to the auditors. Management will identify lessons learned from this audit and will establish a working group to improve timeliness in providing audit artifacts. Through these and other efforts, management will further develop a shared understanding of auditor expectations among stakeholders involved in DO's consolidated financial statement audit.

4. Untimely Recording of the Quarterly GSE Liquidity Preference Increase

Following the initiation of the September 27, 2019 amendment to the Government Sponsored Enterprises (GSE) Senior Preferred Stock Agreement, which resulted in the gradual increase in the liquidation preference, management did not sufficiently update its policies and procedures in a timely manner to include controls to account for the gradual increase per the agreement. Further, management did not update its control checklist timely to include the quarterly journal entry to increase the liquidation preference of each GSE.

Preventive Controls were not operating effectively throughout the period to ensure the Q1 quarterly increase to the GSE liquidation preference was recorded timely. Management identified the unrecorded increase in late January 2020 and subsequently recorded the liquidation preference increase in March 2020. Although the execution of subsequent review controls resulted in the identification of the error, it was not identified in a timely manner. Additionally, management updated its policy, procedures, and control documentation to reflect the liquidation preference increase policies and procedures in March 2020.

As a result of the ineffective operation of the preventive control over the recording of the quarterly liquidation preference increase, the Q1 increase was not recorded timely. Failure to timely record increases to the GSE liquidation preference could result in an understatement of the GSE general ledger and the Investment in GSE or other related financial statement line items and accounts.

Recommendation

We recommend that management strengthen control procedures to ensure policies, procedures, and related control activity documentation are timely updated for continued relevance and effectiveness of key controls based on changes in legislation, policies, and agreements related to GSE activities.

Management Response

While we agree that the lack of update to our policy, procedures, and controls may have prevented us from recording the entry in a timely manner, this error was caught upon our effective execution of detective controls that were designed for this purpose. These controls allowed us to discover and properly record the entry in the following quarter. Given the effectiveness of our detective controls, which occurred well before these transactions would have been reported externally to the public

(annually in November), we do not consider this to be a deficiency that would have resulted in an error in our externally reported financial statements.

KPMG Response

We evaluated the finding noted above, in accordance with auditing standards generally accepted in the United States of America, to conclude that a deficiency in the design of the preventative control exists despite the presence of a detective control.

5. Lack of Appropriate Review of JFICS Year-end Accrual

Management did not appropriately design the control over the calculation of the year-end judgment fund accrual to ensure its completeness and accuracy. The inappropriate design of the control resulted in improper recording of judgment fund claims in FY 2020 that should have been accrued in FY 2019.

As a part of our testing over the Judgment Fund Internet Claims System (JFICS) and Oracle interface control, we identified a judgment fund claim of \$3,808.72 that was approved for payment in FY2019 but was not expensed in USSGL 61000053-Operating/Program Expenses – Other Federal Costs or accrued for in USSGL 2110000-Accounts Payable as of September 30, 2019. Instead, the claim was not recorded in the proper period, resulting as a claim expense in USSGL 61000053-Operating/Program Expenses – Other Federal Costs in FY 2020. After further analysis, we identified additional judgment fund claims that were approved for payment after an 8:00 a.m. cutoff on September 30, 2019, but were then excluded from the year-end accrual because the JFICS Payables Report used by the Bureau of the Fiscal Service (Fiscal Service) to calculate and record the accrual does not include claims approved after 8:00 a.m. on the last day of the month. This resulted in the lack of recording (a total of \$712,714.62) of transactions in the proper period.

Due to the inappropriate design of the judgment fund claim accrual process, misstatements occurred that understated USSGL 61000053-Operating/Program Expenses – Other Federal Costs and USSGL 2110000-Accounts Payable as of September 30, 2019 by \$712,714.62 and overstated USSGL 61000053-Operating/Program Expenses – Other Federal Costs by \$712,714.62 in FY 2020.

Recommendation

Fiscal Service management should design additional policies and procedures around the JFICS accrual control to capture claims approved in JFICS at year-end to ensure the completeness and accuracy of the related account balances.

Management Response

Fiscal Service agrees with the condition and recommendation outlined above resulting in the immaterial misstatement of the year-end judgment fund claim accrual.

To remediate the condition, Fiscal Service management and operational staff met to update policies and procedures to address the completeness and accuracy of the year-end accruals. The updated policies and procedures incorporate design improvements to capture claims that have been approved for payment in the JFICS system as of year-end. This new process will ensure the completeness and accuracy for all JFICS claims at year-end for related account balances.

6. Lack of Documentation of Review Over FMFIA Compliance Testing Results; and Incorrect Compilation on the Statement of Assurance Review Sheet

The Federal Manager's Financial Integrity Act of 1982 (FMFIA) requires federal agencies to establish internal controls to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The Treasury Chief Financial

Officers' Council (CFO Council) has overall governance responsibility for the Treasury-wide internal control program. To achieve this, the Risk and Control Group (RCG) at the Treasury requires that each individual Treasury component prepares and submits the results of their FMFIA assessments annually.

The Department's RCG has in place appropriate control design and guidance to ensure compliance around the FMFIA. However during the year the control was not fully operational to identify and prevent certain errors and missing information from the A-123 results submitted by the Components. Specifically:

- DO:
 - For “Security Program – Gross Cost” control, there is no reference to a specific control objective that addresses the identified risks.
- Deputy Chief Financial Officer (DCFO), which includes Government Sponsored Entity (GSE) and International Monetary Fund (IMF):
 - Management incorrectly concluded on the result of testwork, specifically within transaction results PS-4 (GSE) and PE-28 (IMF). The result was inconsistent with the test work performed.
 - Office of Financial Reporting and Policy – The sample size chosen of two for a monthly control did not sufficiently satisfy the Treasury A-123 implementation guidance, which recommends three tests for a monthly control.
- Financial Crimes Enforcement Network (FinCEN):
 - FinCEN – There is a lack of preparer and reviewer signoff documented within the testwork.
 - FinCEN – There is a lack of documentation around sample selection, specifically the sample size used.
- Fiscal Service:
 - Funds Management Branch (FSM) – Management did not document the test of operating effectiveness of Control FSM AP-1 within their allotted section.
 - FSM – There is incomplete documentation around various controls, namely FSM AC-6 and AC-9, where control objectives are not identified or documented when management is relying on the ARC SSAE 18 report.
- Fiscal Service Debt (FSD):
 - FSD – There is missing documentation around various controls, specifically justification around sample size selection.
- Office of Comptroller of the Currency (OCC):
 - There is missing control documentation regarding justification of sample sizes.
- Annual Approval of Assurance Statement:
 - We noted an incorrect compilation of the Treasury Assurance Statement Review Worksheet. Specifically, the Assurance Statement Review Sheet inappropriately classified the Office of

Privacy, Transparency, and Records as “Unmodified,” when, in fact, it actually expressed a “Modified” Statement of Assurance.

Without proper review over the A-123 testing by RCG, Treasury is at risk for incorrectly assessing its controls over financial reporting, having improper sample selection, or not having adequate support for their conclusions. Furthermore, without proper review and conclusions over the components’ Assurance Statements by RCG, Treasury is at risk for incorrectly assessing its Consolidated Treasury Assurance Statement conclusion as Unmodified.

Recommendation

To assist management in mitigating the risk of potential noncompliance with FMFIA if (1) results of testing were not documented or (2) were not consistently tested by the components, we recommend that management enforce guidance on how to improve A-123 documentation and implementation of internal controls. Additionally, management should perform a more detailed review of the sufficiency of the component submissions, follow up with all inconsistencies, and have documentation readily available to substantiate the conclusion that was reached.

Management Response

Management concurs with the overall finding and plans to update its guidance to require more standardization in documentation and to reinforce proper documentation standards. In addition, we plan to fill vacant positions to ensure we are properly resourced. These actions will enable us to review the documentation more thoroughly and follow up with bureaus on inconsistencies or missing documentation. However, we do not concur with the characterization of two findings. The first finding under the Office of the DCFO states that management incorrectly concluded on the result of test work within transaction results PS-4 (GSE) and PE-28 (IMF). It should be noted that management did not incorrectly conclude on the test work, rather, there was a typo that indicated there were exceptions found during testing when in fact no exceptions were found. The results of the testing omitted the word “no” before “exceptions”, as in “no exceptions were noted.” Next, the first finding under Fiscal Service, states that “management did not document the test of operating effectiveness of Control FSM AP-1 within their allotted section”, however the test of effectiveness was documented within the same test plan. It was labeled AP-2 instead of AP-1. Treasury guidance states “Components may use earlier versions of the risk and control matrix (located in the Treasury Catalogue of Risk and Controls) **or design their own**” (pg. 14). We do not require a specific label for the control.

KPMG Response

As noted in Management’s Response, control documentation was inconsistent which contributed to the identified findings and recommendations noted above.

THE DEPARTMENT OF THE TREASURY
Status of Prior-Year Management Letter Comments

Fiscal Year 2019 Management Letter Comments

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

Fiscal Year 2020 Status – In FY 2020, this finding has been bifurcated in order to separate and better align the responsibilities of FARS and DO IT management. Treasury management notes the remediation of the FARS specific recommendation was completed in March 2020 while the DO IT specific recommendation remains un-remediated as of September 30, 2020.

2. FARS User Accounts Management Needs Improvement

Fiscal Year 2020 Status – Remediated

3. The Process of Compliance over FMFIA Process Could be Improved

Fiscal Year 2020 Status – Reissued in FY 2020 as Finding #6 in Appendix A

4. Appropriate Documentation of the Preparation and Review of Government-wide Cash Core Trial Balance to TIER Reconciliation Needs to be Improved

Fiscal Year 2020 Status – Remediated

5. Appropriate Review of Year-end Balances Submission from the Fiscal Service Funds Management Branch Needs to be Improved

Fiscal Year 2020 Status – Remediated



REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898

Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)

gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:

www.treasury.gov/about/organizational-structure/ig