Audit Report

OIG-25-013

FINANCIAL MANAGEMENT

Management Letter for the Deficiencies in Internal Control over Cash Management Systems at the Bureau of the Fiscal Service Identified during the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2024 and 2023

December 6, 2024

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, 2024

MEMORANDUM FOR TIMOTHY E. GRIBBEN, COMMISSIONER
BUREAU OF THE FISCAL SERVICE

FROM: Shiela Michel /s/
Acting Director, Financial Statement Audits

SUBJECT: Management Letter for the Deficiencies in Internal Control over Cash Management Systems at the Bureau of the Fiscal Service Identified during the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2024 and 2023

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, 2024 and 2023, 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. 24-02, *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 6, 2024, that discusses matters involving deficiencies in internal control over financial reporting that were identified during the audit but were not required to be included in the auditors' report. These matters involved deficiencies in internal control over cash management systems at the Bureau of the Fiscal Service (Fiscal Service). Fiscal Service management's responses to the findings and recommendations are included. These responses were not audited by KPMG. Management will need to include the proposed corrective action completion dates related to the recommendations in the Department of the Treasury's 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.

If you wish to discuss this report, please contact me at (202) 486-1415, or a member of your staff may contact Catherine Yi, Audit Manager, Financial Statement Audits, at (202) 553-7412.

Attachment

cc: Aditi Hardikar
Assistant Secretary for Management

David Lebryk
Fiscal Assistant Secretary

Carole Y. Banks
Deputy Chief Financial Officer

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

December 6, 2024

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

Ms. Aditi Hardikar
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, 2024, 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, a component entity 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, 2024 on our consideration of the Department's internal control over financial reporting in which we communicated a deficiency in internal control that we considered to be a significant deficiency for the Department as a whole.

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 at the Bureau of the Fiscal Service (Fiscal Service), which are described in Appendix I. Appendix II presents the status of the prior year comments.

Fiscal Service's responses to the findings identified in our audit are described in Appendix I. Fiscal Service'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 over cash management systems at the Bureau of the Fiscal Service identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Appendix I

THE DEPARTMENT OF THE TREASURY

Management Letter comments

1) Untimely PAM Mainframe Terminated User Access Removal

The Bureau of the Fiscal Service (Fiscal Service) management did not properly implement the control for removing PAM Mainframe access for terminated/resigned users within two business days of their effective separation date. Specifically, one user had an effective separation date of March 31, 2024, and wasn't removed from the PAM Mainframe Operating System until April 18, 2024 (14 business days). Fiscal Service management did not enforce accountability of individuals performing logical access control responsibilities and monitor the operating effectiveness of controls for removing logical access for separated individuals in a timely manner.

Without timely removal of system access for terminated users, the risk exists that the separated individual or another individual with knowledge of the separated person's logon credentials could use the unauthorized access to the PAM zOS Mainframe system to perform inappropriate user activity, which could adversely impact the integrity of the PAM system and its financial payment data.

Recommendation

We recommend that Fiscal Service management:

1. Reinforce policy requirements (through training or other means) for removing logical access of terminated and transferred Fiscal Service employees and contractors within 2 business days of their separation date, and
2. Perform ongoing monitoring to hold responsible control performers accountable for timely completion of such control activities.

Management Response

Fiscal Service management concurs with the findings and recommendations as stated above.

2) Splunk User Access Review for CAIA Not Implemented

The Bureau of the Fiscal Service (Fiscal Service) management did not properly implement the Authentication Services (AS) quarterly user access review and recertification control to include all privileged users. Specifically, the AS Splunk administrators supporting CAIA were not included in the review. Fiscal Service management did not evaluate changes in the use of information technology and implement new or updated policies and controls to address new logical access objectives and risk in a timely manner.

Without a review and recertification of AS Splunk administrator access for CAIA, the risk exists that individuals with unauthorized privileged access to Splunk go undetected. Such access could allow the user to perform inappropriate privileged activity, which could adversely impact the integrity and availability of key user access and activity reports relied upon by management for connected applications such as CARS and PAM.

Recommendation

We recommend that Fiscal Service implement policies and controls for performing a user access review and recertification of AS Splunk Administrators supporting CAIA on a quarterly basis.

Management Response

Fiscal service management concurs with the findings and recommendations as stated above.

3) PAM Mainframe Privileged User Access Review Control Weakness

The Bureau of the Fiscal Service (Fiscal Service) management did not properly implement the control for reviewing and recertifying privileged PAM Mainframe Operating System and DB2 access. Specifically, the review was performed solely by the System Programmer who was not independent of the access being reviewed, and the secondary reviewer, the Mainframe Branch Manager, did not review and approve the System Programmers access and results of the review after completion by the System Programmer. Fiscal Service management did not divide or segregate key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. Additionally, Fiscal management did not enforce accountability of individuals logical access control responsibilities.

Without implementing an independent review of user's access, the risk exists that the reviewer recertifies or modifies their access to something that is unauthorized or in excess of the access needed for their job responsibilities. Such access could allow the user to perform inappropriate activity, which could adversely impact the PAM system and its financial payment data.

Recommendations

We recommend that Fiscal Service management:

1. Implement proper segregation of duties to ensure that an independent review of all user's access is performed as part of the semi-annual PAM Mainframe privileged user access review, and
2. Enforce accountability of individuals performing user access review control responsibilities in accordance with policies and procedures.

Management Response

Fiscal Service concurs that the semi-annual mainframe recertification was not reviewed and approved as designed which if implemented would have ensured proper segregation of duties during the review. To address this issue, Fiscal Service will ensure the recertification is completed and approved through automation and/or additional oversight where feasible.

Appendix II

THE DEPARTMENT OF THE TREASURY

Status of Prior-Year IT Deficiencies for Government-wide Cash and Treasury Managed Accounts

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2024 Status**
FY 2019 – 7) Lack of audit log policies and procedures for payment system production database and production UNIX servers and lack of database security audit log reviews.	***Partially Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2024 Status
Finalize policies and procedures to review audit logs of production IBM Database 2 (DB2) servers. (FY 2019 recommendation #37)	FS management implemented audit logging and monitoring via Splunk on 3/6/2024.	We determined that the statuses of these recommendations remained open for the period October 1, 2023 through March 6, 2024 based on our assessment that Fiscal Service management implemented corrective actions via Splunk on March 6, 2024. Due to the timing of the remediation, KPMG considers this finding partially open and will determine if remediation has fully occurred in subsequent audit years.	Partially Open
Implement an oversight process to ensure that designated Fiscal Service management: a. Reviews the security logs for the UNIX and DB2 servers hosting the PIR, JFICS, and SPS applications on a pre-defined frequency, as indicated in the BLSR. b. Formally documents completion of their reviews and any escalations to the Information System Security Officer (ISS), and c. Retains the audit logs and documentation of its reviews for 18 months, as required by the BLSR. FY19 Rec #38			Partially Open

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2024 Status
Periodically review Fiscal Service management's implementation and operation of the review the security audit logs for the UNIX and DB2 servers hosting the PIR, JFICS, and SPS applications to determine that Fiscal Service management completes the reviews on a pre-defined basis, documents completion of the reviews and escalations, and maintains such documentation. (FY 2019 recommendation #39)			Partially Open
Establish an effective enforcement process or mechanism to ensure that (a) UNIX and DB2 events and monitoring controls are followed, and (b) Fiscal Service management has confidence it consistently reviews for potential unauthorized or inappropriate activity. (FY 2019 recommendation #40)			Partially Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	FY 2024 Status
FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2024 Status
Develop and implement documentation to assign responsibility for ensuring adequacy of UNIX and database security and baseline settings. (FY 2019 Recommendation #62)	Fiscal Service management's corrective actions are planned to be implemented after FY 2024. During internal review Fiscal Service determined that additional work was required to satisfy the entirety of the recommendations.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management plans to implement corrective actions after FY 2024.	Open
Update existing UNIX and database configuration security baseline documents to ensure that these documents fully incorporate and enforce the components of the DISA STIGs. Management should document any deviations from the STIGs, and note compensating controls that mitigate the security risk to an acceptable level. (FY 2019 Recommendation #63)			Open
Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual UNIX and database settings against the security configuration baselines. (FY 2019 Recommendation #64)			Open
Provide logging and monitoring of security related events to include the retention of evidence of reviews performed. (FY 2019 Recommendation #65)			Open

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2024 Status
Develop a baseline of essential security settings and specify that baseline as the standard to be observed. (FY 2019 Recommendation #66)			Open
Implement corrective actions to address all vulnerabilities associated with the baseline enforcement to include removing the three default user accounts on UNIX servers. (FY 2019 Recommendation #67)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding – UNIX Mid-Tier systems	**FY 2024 Status**
FY 2020 Finding – 5) Information System Component Inventory Needs Improvement (UNIX Mid-Tier)	***Open***

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2024 Status
Perform a review of the current system environment against the CMDB. (FY 2020 recommendation #10)	Fiscal Service management's corrective actions are planned to be implemented after FY 2024. During internal review Fiscal Service determined that additional work was required to satisfy the entirety of the recommendations.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management plans to implement corrective actions after FY 2024.	Open
Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for monitoring and updating the CMDB. (FY 2020 recommendation #11)			Open
Update policy and procedures related to the above recommendations and disseminate the documentation to enforce such policy and procedures. (FY 2020 recommendation #12)			Open

LIST OF ABBREVIATIONS

Abbreviations	Definition
BLSR	Baseline Security Requirements
CMDB	Configuration Management Database
DB	Database
DB2	IBM Database 2
DISA	Defense Information Systems Agency
EITI	Enterprise Information Technology Infrastructure
Fiscal Service	Bureau of the Fiscal Service
FY	Fiscal Year
GWC	Government-Wide Cash
ISS	Information Security Services
IT	Information Technology
JFICS	Judgment Fund Internet Claim System
OMB	Office of Management and Budget
PIR	Payment Information Repository
SPS	Secure Payment System
STIG	Security Technical Implementation Guide
TMA	Treasury Managed Accounts
Department	Department of the Treasury

Notes

SPS is an automated system for payment schedule preparation and certification. The system provides positive identification of the certifying officer, who authorizes the voucher, and ensures the authenticity and certification of data. The SPS application provides a mechanism by which government agencies can create payment schedules in a secure fashion.

PIR is a centralized information repository for Federal payment transactions.

UNIX operating system is included in the EITI boundary, also PIR application resides within the UNIX. Therefore, the EITI SSP is also applicable to UNIX and PIR.

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/