Audit Report

OIG-24-009

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 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 TIMOTHY E. GRIBBEN, COMMISSIONER
BUREAU OF THE FISCAL SERVICE

FROM: Ade Bankole /s/
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 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 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 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) 927-5329, or a member of your staff may contact Mark S. Levitt, Audit Manager, Financial Statement Audits, at (202) 439-6138.

Attachment

cc: Anna Canfield Roth
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

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 – Troubled Asset Relief Fund, 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 did not identify any new deficiencies in internal control over cash management systems at the Bureau of the Fiscal Service (Fiscal Service). Appendix I presents the status of the prior year comments and Fiscal Service's responses. 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

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 2023 Status
FY 2019 – 1) Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources. (GWC and TMA)	***Closed***
FY 2019 – 2) Mainframe security software configuration baseline settings have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access.	***Closed***
FY 2019 – 3) Excessive privileged access that violates the principle of least privilege is allowed on the Mainframe.	***Closed***
FY 2019 Finding– 5) Mainframe security control documentation needs improvement. (GWC and TMA)	***Closed***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2023 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.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2023 Status
Finalize policies and procedures to review audit logs of production IBM Database 2 (DB2) servers. (FY 2019 recommendation #37)	Fiscal Service management's corrective actions are planned to be implemented after FY 2023. Logging is being implemented by Fiscal Service following the required enterprise logging levels outlined by OMB.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management implemented corrective actions in late FY 2023 and were not operating for the majority of FY 2023.	Open
Implement an oversight process to ensure that designated Fiscal Service personnel: 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			Open

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2023 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)			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)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2023 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 2023 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 2023. 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 implemented corrective actions in late FY 2023 and were not operating for the majority of FY 2023.	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 2023 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

Appendix I

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding – UNIX Mid-Tier systems	**FY 2023 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 2023 Status
Perform a review of the current system environment against the CMDB. (FY 2020 recommendation #10)	Fiscal service is preparing a new service management platform called Enterprise Service Management (ESM) that will replace the existing IT service management platform. A new CMDB utilizing new data model will be established as a part of this effort. Additionally, Fiscal Service management's corrective actions are planned to be implemented after FY 2023.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management implemented corrective actions in late FY 2023 and were not operating for the majority of FY 2023.	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.

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/