



Audit Report



OIG-26-017

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 Year 2025

February 13, 2026

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

February 13, 2026

**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 Year 2025

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, 2025, and for the year 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 February 13, 2026, 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.

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, Manager, Financial Statement Audits, at (202) 553-7412.

Attachment

cc: John W. York
Assistant Secretary for Management

Gary Grippo
Acting Fiscal Assistant Secretary

Carole Y. Banks
Deputy Chief Financial Officer



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

February 13, 2026

Loren J. Sciarba
Deputy Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

John W. York
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, 2025, 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 January 27, 2026 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 deficiency in internal control at the Bureau of the Fiscal Service (Fiscal Service), which is described in Appendix I. Appendix II presents the status of the prior year's 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.



Loren J. Sciorba
John W. York
Department of the Treasury
February 13, 2026
Page 2 of 2

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

THE DEPARTMENT OF THE TREASURY

Management Letter comment

1. Untimely Secure Payment System (SPS) Application Terminated User Access Removal

The Bureau of Fiscal Service (Fiscal Service) management did not properly implement the control for removing SPS Application access for terminated/resigned users within two business days of their effective separation date, in accordance with the SPS System Security Plan and Federal Security Assessment Tool (FSAT). Specifically, four SPS users retained access beyond two business days of their effective separation date. 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 individual's logon credentials could leverage the unauthorized access to the SPS application to perform inappropriate user activity, which could adversely affect or impact the integrity of the SPS system and its financial payment data.

Recommendations

We recommend that Fiscal Service management:

- a. 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
- b. Perform ongoing monitoring to hold responsible control operators accountable for timely completion of such control activities.

Management Response

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

THE DEPARTMENT OF THE TREASURY

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

Deficiencies Included in the Fiscal Year (FY) 2024 Management letter	FY 2025 Status
<i>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.</i>	<i>Closed</i>
<i>FY 2024 – 1) Untimely PAM Mainframe Terminated User Access Removal</i>	<i>Closed</i>
<i>FY 2024 – 2) Splunk User Access Review for CAIA Not Implemented</i>	<i>Closed</i>
<i>FY 2024 – 3) PAM Mainframe Privileged User Access Review Control Weakness</i>	<i>Closed</i>

Appendix II

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	FY 2025 Status
<i>FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.</i>	<i>Partially Open</i>

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2025 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 represented, and provided information to the auditors, that they implemented corrective actions to remediate the prior-year Unix Mid-Tier Baseline Process over control weakness. The corrective actions taken by Fiscal Service management remediated this issue effective March 2025	Management remediated the recommendations in FY2025. Due to the timing of the remediation, KPMG considers this finding partially open and will determine if remediation has fully occurred in the subsequent audit years	Partially 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)			Partially 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)			Partially Open
Provide logging and monitoring of security related events to include the retention of evidence of reviews performed. (FY 2019 Recommendation #65)			Partially Open

Appendix II

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2025 Status
Develop a baseline of essential security settings and specify that baseline as the standard to be observed. (FY 2019 Recommendation #66)			Partially 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)			Partially Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding – UNIX Mid-Tier systems	FY 2025 Status
<i>FY 2020 Finding – 5) Information System Component Inventory Needs Improvement (UNIX Mid-Tier)</i>	<i>Open</i>

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2025 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 2025. During internal review Fiscal Service Management 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 2025.	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
CMDB	Configuration Management Database
DISA	Defense Information Systems Agency
EITI	Enterprise Information Technology Infrastructure
Fiscal Service	Bureau of the Fiscal Service
FSAT	Federal Security Assessment Tool
FY	Fiscal Year
IT	Information Technology
PIR	Payment Information Repository
SPS	Secure Payment System
STIG	Security Technical Implementation Guide
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.

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/>