



Audit Report



OIG-24-019

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Bureau of Engraving and Printing's Financial Statements for Fiscal Years 2023 and 2022

December 20, 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 20, 2023

**MEMORANDUM FOR CHARLENE E. WILLIAMS, ACTING DIRECTOR
BUREAU OF ENGRAVING AND PRINTING**

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

SUBJECT: Management Letter for the Audit of the Bureau of Engraving
and Printing's Financial Statements for Fiscal Years 2023 and
2022

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 Bureau of Engraving and Printing (BEP) 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 December 19, 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 general information technology controls. BEP 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 Shiela Michel, Manager, Financial Statement Audits, at (202) 486-1415.

Attachment

This Page Intentionally Left Blank



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

December 19, 2023

The Deputy Inspector General, Department of the Treasury and
The Acting Director of the Bureau of Engraving and Printing, Department of the Treasury:

To the management of the Bureau of Engraving and Printing:

In planning and performing our audit of the financial statements of the Bureau of Engraving and Printing (the Bureau) 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, and the Office of Management and Budget (OMB) Bulletin No. 24-01, *Audit Requirements for Federal Financial Statements*, we considered the Bureau'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 financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Bureau's internal control. Accordingly, we do not express an opinion on the effectiveness of the Bureau's internal control.

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 December 19, 2023 on our consideration of the Bureau's internal control over financial reporting.

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 described in Appendix A. Appendix B presents the status of the prior year deficiencies.

The Bureau's responses to the deficiencies identified in our audit are outlined in Appendix A. The Bureau's responses were not subjected to the auditing procedures applied in the audit of the 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 BUREAU OF ENGRAVING AND PRINTING

Management Letter Comments

1) LAN WAN Password Weaknesses

The Bureau's Local Area Network/Wide Area Network (LAN WAN) users authenticate to the network with a Personal Identity Verification (PIV) card, with the exception of those users granted temporary PIV exemptions. PIV exceptions can occur for a number of reasons, such as a lost or stolen PIV card. Users with PIV exemptions are able to access the network with a username and password instead of a PIV card.

In fiscal year (FY) 2023, we determined that the Active Directory (AD) password settings enforced for LAN WAN users with PIV exemptions were not configured in accordance with the Bureau's policy requirements.

This condition occurred due to a lack of an effective account management process for operating systems in place and management did not ensure that the requirement for operating systems was implemented for the AD. Management was aware of this deviation but prioritized the timeliness of implementing an updated operating system baseline over the remediation of this deficiency.

Weaknesses in password configuration settings increases the risk of systems and data being compromised, which could allow an individual to perform unauthorized activities that would impact the functionality of the system and the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that management update LAN WAN password configuration settings to comply with policy requirements or formally document a risk acceptance with mitigating controls.

Management Response

Management concurred with the finding and recommendation.

2) User Inactivity Monitoring Needs Improvement

Since FY 2020, we reported that management did not disable inactive user accounts on the Bureau's Local Area Network/Wide Area Network (LAN WAN) in accordance with policy.

In FY 2023, we determined that deficiencies continued to exist in the implementation of controls to effectively manage users accounts. Specifically, we identified user accounts that were not compliant with the Bureau's policy on network account inactivity.

Corrective actions for this prior year finding were not completed during FY 2023, which caused the weakness to continue. Management indicated during the prior year audit that user accounts were moved to an Active Directory (AD) Organizational Unit (OU) that was not being captured in the automated script used to identify and disable LAN WAN accounts after 30 days of inactivity. Additionally, the Bureau's management indicated that a manual review process was developed to address the weakness.

Untimely disabling of inactive user accounts increases the risk of users retaining unauthorized or inappropriate system access. Such access could allow an individual to advertently or inadvertently perform unauthorized activities that would impact the functionality of the system and compromise the confidentiality, integrity, and availability of its data.

Recommendation

We recommend that management:

1. ensure that all AD OUs are captured in the automated script used to identify and disable LAN WAN accounts after 30 days of inactivity,
2. enforce existing requirements to disable inactive LAN WAN user accounts in accordance with the threshold established by policy, and
3. document and implement procedures around the manual review process used to identify accounts that have not been logged in to for over 30 days.

Management Response

Management concurred with the finding and recommendations.

THE BUREAU OF ENGRAVING AND PRINTING
Status of Prior Year Management Letter Comments

Fiscal Year 2022 Management Letter Comments

1. Vulnerability Management Weakness
Fiscal Year 2023 Status – Closed
2. User Inactivity Monitoring Needs Improvement
Fiscal Year 2023 Status – Re-issued (See Appendix A.2)
3. Ineffective Controls Over the Cash Balance Reconciliation
Fiscal Year 2023 Status – Closed
4. Ineffective Controls over the Review of Capital Projects in Construction in Progress
Fiscal Year 2023 Status – Closed

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/>