Audit Report

OIG-26-020

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Bureau of Engraving and Printing's Financial Statements for Fiscal Year 2025

February 26, 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 26, 2026

MEMORANDUM FOR PATRICIA A. SOLIMENE, DIRECTOR
BUREAU OF ENGRAVING AND PRINTING

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

SUBJECT: Management Letter for the Audit of the Bureau of Engraving and Printing's Financial Statements for Fiscal Year 2025

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, 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 23, 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 general information technology controls. BEP management's responses to the recommendations is included. The 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 Felicia Silver, Acting Manager, Financial Statement Audits, at (771) 210-6004.

Attachment

BUREAU OF ENGRAVING AND PRINTING

Management Letter

For the Year Ended September 30, 2025

BUREAU OF ENGRAVING AND PRINTING

Management Letter

For the Year Ended September 30, 2025

Table of Contents

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

February 23, 2026

Deputy Inspector General
Department of Treasury
Washington, DC

Director
Bureau of Engraving and Printing
Washington, DC

To the Deputy Inspector General and Director:

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, 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, and in accordance with the Office of Management and Budget (OMB) Bulletin No. 24-02, *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 February 23, 2026 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 deficiencies in internal control which are summarized in Appendix A. Appendix B presents the status of the prior year deficiency.

The Bureau's written responses to the deficiencies identified in our audit are described Appendix A. The Bureau's written responses were not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on them.

This 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

BUREAU OF ENGRAVING AND PRINTING

Fiscal Year 2025 Management Letter Comments

Information Technology (IT) Deficiencies

A-1 LAN WAN Password Weaknesses

Since fiscal year (FY) 2023, we reported that BEP 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 FY 2025, we determined that the deficiencies continued to exist in the implementation of the Active Directory (AD) password settings enforced for LAN WAN users with PIV exemptions not being configured in accordance with BEP policy requirements.

The United States Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated September 2014, states:

> **11.11** Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. […]

Corrective actions for the prior year findings were not completed during FY 2025, which caused the weakness to continue to exist. BEP management indicated that password settings for select operating systems due to the substantial number of applications that are either legacy or created in-house related to manufacturing equipment and the need for careful change management planning, testing, and implementation to avoid negative impact to the BEP mission.

Additionally, the password complexity for the AD was configured to 'Enabled' but this configuration did not require all categories, and management did not note this system limitation as being permissible within the policy requirements, which caused this configuration setting to be out of compliance with policy. BEP management stated [redacted].

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 BEP 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.

A-2 Weakness in Timely Removal of Oracle Manufacturing Support Suite (MSS) Terminated User Access

We determined that BEP management did not remove Oracle Manufacturing Support Suite (MSS) user accounts for terminated users in accordance with BEP policy. Specifically, four of 15 sampled Oracle MSS user accounts were not disabled within one business day of their effective termination date.

United States Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government (Green Book)*, dated September 2014, states:

Enforce Accountability 5.03, "Management holds entity personnel accountable for performing their assigned internal control responsibilities. The oversight body, in turn, holds management accountable as well as the organization as a whole for its internal control responsibilities."

Internal Control System Monitoring 16.05, "Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions."

BEP Minimum Standard Parameters, Version 6.4, dated March 7, 2024, control AC-2: Account Management and PS-4: Personnel Termination states:

“AC-2: Account Management

Control: […]

a. Notify account managers and [BEP SOC] within:

1. [1 business day] when accounts are no longer required;

2. [24 hours] when users are terminated or transferred; and

3. [1 business day] when system usage or need-to-know changes for an individual.” […]”

“PS-4: Personnel Termination

Control:

a. Disable system access [within 1 hour];

b. Terminate or revoke any authenticators and credentials associated with the individual;” […]

“PS-4(2): Personnel Termination | Automated Actions

Use [Remedy, HRConnect and/or email] to notify [OITO, BEP SOC and Cyber Operations Division Team] of individual termination actions.”

United States National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, dated September 2020, states:

“AC-2: Account Management:

Control: […]

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

1. [Assignment: organization-defined time period] when accounts are no longer required;

2. [Assignment: organization-defined time period] when users are terminated or transferred; and

3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual." […]

"PS-4: Personnel Termination

Control: Upon termination of individual employment:

a. Disable system access within [Assignment: organization-defined time period];

b. Terminate or revoke any authenticators and credentials associated with the individual;" […]

"PS-4(2): Personnel Termination | Automated Actions

Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources]."

Per inquiry of BEP management, BEP human resources (HR) team did not effectively monitor the timely initiation of personnel termination requests within the HR system, which resulted in delayed workflow to remove the terminated user accounts within one business day of the employees' effective termination date.

Untimely removal of terminated users' access to BEP's Oracle MSS increases the risk of unauthorized access to the Oracle MSS application, which could lead to an increased risk of compromise in data confidentiality, integrity, and availability.

Recommendation

We recommend that BEP management reinforce and monitor policy requirements for initiating personnel termination requests in a timely manner to help remove logical access of terminated employees and contractors within the required timeframe.

Management Response

Management concurred with the finding and recommendation.

Appendix B

BUREAU OF ENGRAVING AND PRINTING

Status of Prior Year Management Letter Comment

Fiscal Year 2024 Management Letter Comment	Fiscal Year 2025 Status
1) LAN WAN Password Weaknesses	Re-issued, A-1

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/