Audit Report

OIG-21-012

FINANCIAL MANAGEMENT

Management Letter for the Audit of the United States Mint's Financial Statements for Fiscal Years 2020 and 2019

December 8, 2020

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 8, 2020

MEMORANDUM FOR DAVID J. RYDER, DIRECTOR
UNITED STATES MINT

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the United States Mint's Financial Statements for Fiscal Years 2020 and 2019

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 United States Mint as of September 30, 2020 and 2019, 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 (OMB) Bulletin No. 19-03, *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 7, 2020, that discusses certain matters involving deficiencies in information technology controls that were identified during the audit, but not required to be included in the auditors' report.

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) 927-0009, or a member of your staff may contact Ade Bankole, Manager, Financial Audit, at (202) 927-5329.

Attachment

This Page Intentionally Left Blank

THE UNITED STATES MINT

Management Letter

For the Year Ended September 30, 2020

The United States Mint
Management Letter

For the Year Ended September 30, 2020

Table of Contents

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

December 7, 2020

Deputy Inspector General
Department of the Treasury
875 15th Street, NW,
Washington, DC 20005

Director
United States Mint
801 9th Street, NW
Washington, DC 20001

Gentlemen:

In planning and performing our audit of the financial statements of the United States Mint, as of and for the years ended September 30, 2020 and 2019, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements,* we considered the United States Mint's internal control over financial reporting (internal control) as a basis for designing our auditing 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 United States Mint's internal control. Accordingly, we do not express an opinion on the effectiveness of the United States Mint'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 7, 2020 on our consideration of the United States Mint'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 prior year comments.

The United States Mint's responses to the findings identified in our audit are described in Appendix A. The United States Mint'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

Appendix A

THE UNITED STATES MINT

Fiscal Year 2020 Management Letter Comments

Information Technology (IT) Findings

A-1 User Account Management for WAN/LAN Needs Improvement

In the prior year, we reported deficiencies with the Mint's user account management controls over the General Support System (GSS) Wide Area Network (WAN)/Local Area Network (LAN). Documentation supporting new access approval for certain users was unavailable.

During Fiscal Year (FY) 2020, we continued to identify testing exceptions over the WAN/LAN new user authorization processes. Specifically, we noted the following:

- One out of 15 new WAN/LAN users had their account enabled prior to receiving manager approval.
- One out of 15 new WAN/LAN users did not have an access approval form.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 Account Management states:

> "The organization:
> [...]
> e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts"

The *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States, Principal 11 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. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.
>
> 11.14 Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when different information technology elements are connected to each other."

Mint management did not properly enforce the completion of access request forms, with documented approvals prior to granting users access to the system, or the retention of such documentation supporting the approval.

Ineffective controls over access to programs and data, increases the risk of unauthorized access to the systems, which could lead to a compromise in data confidentiality, integrity, and availability.

We recommend that Mint management re-enforce requirements to control performers to ensure that new or modified user accounts are approved prior to being enabled and that documentation supporting the approval is retained.

Management Response:

Management concurs with the finding.

A-2 Timely Removal of Terminated Users from the Mint Network Needs Improvement

In the prior year, we reported a deficiency with the Mint's access removal process. Our test results found that the Mint GSS WAN/LAN user accounts had gone unused for more than 90 days and were not disabled. Furthermore, some users who were terminated still maintained an active account in WAN/LAN. Management took corrective action to remediate this prior year deficiency by updating the existing information system security policies and plans for documenting the established timeframe for management to remove user accounts associated with terminated employees and contractors. Additionally, Mint management implemented a configuration within the GSS WAN/LAN system to automatically disable accounts that had been inactive for over 90 days.

During FY 2020, we continued to identify instances where access of terminated users was not removed timely from Mint's systems. Specifically, we noted that the access of two terminated non-privileged users was not removed (disabled) in the Mint GSS WAN/LAN within 5 business days from notice of termination.

The NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* states:

> AC-2 Account Management
> "The organization:
> […]
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];"
> PS-4 Personnel Termination
> "The organization, upon termination of individual employment:
> a. Disables information system access within [Assignment: organization-defined time period];
> b. Terminates/revokes any authenticators/credentials associated with the individual;"

United States Department of the Treasury (Treasury) Directive Publication (TD P) 85-01, Version 3.0.3, states:

"2.12 Managers and Supervisors

> Managers and supervisors shall---
> […]
> 4) Notify SOs [aka system owners] to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies and procedures."

Access Management Policy for Mint Information Systems, dated April 10, 2020, states:

Section 3.4, Termination:
"Non-privileged user accounts must be disabled by ITD within 5 business days of notice of termination. Privileged user accounts must be disabled within 1 business day of notice of termination."

Mint management established a timeframe for control performers to remove user accounts associated with terminated employees and contractors, however, the Mint did not properly implement and enforce the new timeframe amongst the control performers to ensure that the terminated staff accounts are removed in the required timeframe, as per Mint's updated policy.

Ineffective controls over access to programs and data, increases the risk of unauthorized access to the systems, which could lead to a compromise in data confidentiality, integrity, and availability.

We recommend that Mint management enforce termination and transfer procedures to remove system access of terminated or transferred employees and contractors in a timely manner from the network and applications managed by the Mint or by its service providers.

Management Response:

Management concurs with the finding.

A-3 Timely Removal of Terminated Users from Oracle Federal Financial and WebTA Needs Improvement

Mint procures financial accounting services from the Bureau of the Fiscal Service's (Fiscal Service) Administrative Resource Center (ARC) in Parkersburg, WV. Mint utilizes ARC's Oracle Financial system as its core financial management system and general ledger and the WebTA system as its timekeeping system. On an annual basis, ARC obtains an independent Systems and Organization Controls (SOC) 1, Type II, report over ARC's IT and business process controls supporting the Oracle Federal Financial and WebTA environment. In this report, ARC includes the complementary customer agency controls that the Mint should implement locally in order to rely on the SOC 1 report. In the FY 2020 ARC SOC 1 report, there is a complementary customer agency control that directs the Mint to notify the ARC in a timely manner when employees and contractors separate from the Mint.

In the prior year, we reported a deficiency regarding Mint management not notifying the ARC Service Desk Staff of the need to remove the access of certain terminated staff from the Oracle Federal Financial system.

During FY 2020, we continued to identify instances where Mint management did not notify the ARC Service Desk Staff of the need to remove the access of terminated staff from the Oracle Federal Financial system and WebTA system in a timely manner. Specifically, we noted the following:

- For one terminated staff with a separation date of April 30, 2020, the Mint did not request the removal of access from the Oracle Federal Financial system until June 6, 2020.
- For one terminated staff with a separation date of June 6, 2020, the Mint had not requested the removal of access from the WebTA system as of July 22, 2020.

The NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> AC-2 Account Management
> "The organization:
> […]
> g. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];"
>
> PS-4 Personnel Termination
> "The organization, upon termination of individual employment:
> a. Disables information system access within [Assignment: organization-defined time period];
> b. Terminates/revokes any authenticators/credentials associated with the individual;"

Report on the Bureau of the Fiscal Service Administrative Resource Center's Description of its Financial Management Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2019 to June 30, 2020 Complementary Customer Agency Controls, states: "Notify ARC timely regarding exiting employees"

TD P 85-01, Version 3.0.3, states:

"2.12 Managers and Supervisors

> Managers and supervisors shall---
> […]
> 4) Notify SOs [, aka system owners] to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies and procedures."

Access Management Policy for Mint Information Systems, dated April 10, 2020, states:

> Section 3.4, Termination:
> "Non-privileged user accounts must be disabled by ITD within 5 business days of notice of termination. Privileged user accounts must be disabled within 1 business day of notice of termination."

Mint management has not established procedures, to include a required timeframe, for notifying the ARC Service Desk Staff of the need to remove the access of terminated staff from the Oracle Federal Financial system and the WebTA system so that they can be removed in a timely manner, in accordance with Mint and Treasury policy.

Ineffective controls over access to programs and data, increases the risk of unauthorized access to the systems, which could lead to a compromise in data confidentiality, integrity, and availability.

We recommend that Mint management implement and enforce procedures, that include a timeframe requirement, for notifying service providers, such as ARC, of terminated or transferred Mint employees and contractors, so that their access can be removed from applications hosted or managed by the service organizations in a timely manner.

Management Response:

Management concurs with the finding.

Appendix B

THE UNITED STATES MINT

Status of Prior Year Management Letter Comments

Fiscal Year 2019 Management Letter Comments	Fiscal Year 2020 Status
IT Findings	
A-1 User Account Management for WAN/LAN and OMS II Needs Improvement	Re-issued, A-1
A-2 Timely Removal of Inactive Users from the Mint Network Needs Improvement	Re-issued, A-2
A-3 Timely Removal of Terminated Users from Oracle Federal Financial System Needs Improvement	Re-issued, A-3
A-4 HRConnect User Account Recertification Needs Improvement	Closed
A-5 HRConnect User Account Management Needs Improvement	Closed
Non-IT Findings	
A-6 Untimely Review of the Open Obligations Report	Closed
A-7 Insufficient Controls over the Accounting and Reporting of New Lease Obligations	Closed
A-8 Insufficient Review Controls over the Year-end Accruals Process	Closed

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig