Audit Report

OIG-18-026

FINANCIAL MANAGEMENT

Management Letter for the Audit of the United States Mint's Fiscal Years 2017 and 2016 Financial Statements

December 12, 2017

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 12, 2017

**MEMORANDUM FOR DAVID A. MOTL, ACTING DEPUTY DIRECTOR
UNITED STATES MINT**

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the United States Mint's Fiscal Years 2017 and 2016 Financial Statements

I am pleased to transmit the attached subject management letter. Under a contract monitored by our office, KPMG LLP (KPMG), an independent certified public accounting firm, audited the financial statements of the financial statements of the United States Mint as of September 30, 2017 and 2016, 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. 17-03, *Audit Requirements for Federal Financial Statements*, and the Government Accountability Office/President's Council on Integrity and Efficiency *Financial Audit Manual*.

As part of its audit, KPMG issued the attached management letter dated December 8, 2017, that discusses certain matters involving internal control deficiencies and other operational matters that were identified during the audit, but were not required to be included in the auditors' reports.

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 with respect to this management letter.

Should you have any questions, please contact me at (202) 927-0009, or Ade Bankole, Manager, Financial Audit, at (202) 927-5329.

Attachment

THE UNITED STATES MINT

MANAGEMENT LETTER

FOR THE YEAR ENDED SEPTEMBER 30, 2017

THE UNITED STATES MINT
MANAGEMENT LETTER

FOR THE YEAR ENDED SEPTEMBER 30, 2017

TABLE OF CONTENTS

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

December 8, 2017

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

Acting Deputy 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 (Mint), as of and for the years ended September 30, 2017 and 2016, 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. 17-03, *Audit Requirements for Federal Financial Statements,* we considered the Mint's internal control over financial reporting (internal control) as a basis for designing our auditing procedures 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 Mint's internal control. Accordingly, we do not express an opinion on the effectiveness of the Mint's internal control.

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 noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Appendix A. Appendix B presents the status of prior year comments.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Mint's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The Mint's responses to the deficiencies identified in our audit are described in Appendix A. The 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 comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

General IT Controls

A-1 Controls over User Account Management Should be Strengthened

During the FY 2016 audit, we reported a deficiency related to Mint's user account management controls. Our test results found that Wide Area Network (WAN)/Local Area Network (LAN) and Order Management System (OMS) II user accounts were created prior to being properly approved by Mint management. In addition, an OMS II user requested access for himself, and additional manager or supervisor approval was not obtained.

During the FY 2017 audit, we noted that for one out of 15 WAN/LAN user accounts tested, Mint management established the user accounts prior to the user's access being formally approved. For OMS II, management could not locate the completed access approval forms for the following OMS II subsystems:

- One of 15 iCommerce Agent module new users
- Three of 15 Order Management Suite module new users
- One of one NCR Counterpoint users module new users
- Two of two SalesForce Commerce Cloud module new users

Additionally, one inactive test account was not disabled in accordance with Mint policy.

The following Mint, Department of the Treasury (Treasury), and National Institute of Standards and Technology (NIST) security standards and guidelines establish requirements over user access:

WAN/LAN System Security Plan (SSP), Version 9.3, Control AC-2, states:

> Account management Procedures directs that information systems must be configured to ensure that no user is allowed access to an information system or resource (for example, transaction, data, and process) unless authorized by the appropriate manager.

Priority Fulfillment Services Web (PFSweb) Access Control Policy, states:

> Any system access request must be submitted by the individual, or the hiring manager, requesting the access through PFSweb's help desk via the PFSweb Fusion ticketing system. All access must detail the system, access level being requested and reason for access. All requested for access must be approved by the PFSweb area manager and then approved by a PFSweb human resource representative. This cannot be approved by the individual initiating the access request. The human resource representative will validate that the individual user access that is being requested has been approved for the requested access level by the PFSweb area manager, any qualifying third parties and any further parties as required by any client agreement with PFSweb. Once approval is received by the PFSweb area manager and the PFSweb human resource department, the help desk will then assign the ticket to the administrator for the system access that is being requested. All access requests must be closed two business days after approval is received.

Mint Wiki *Network Account Disabling and Removal Procedures,* states:

> Test Accounts:
>
> ITS Data Center is responsible for disabling, archiving, and deleting test accounts. After a test account has been inactive for 30 days, submit a ticket to disable the account and remove the account from all applicable servers.

Treasury Directive Publication (TD P) 85-01, Version 3.0.1, Control AC-2, states:

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

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2, states:

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

Management did not always monitor the Mint employees' compliance with WAN/LAN SSP, PSFweb Access Control policy, and Mint security policy to ensure that users are approved prior to obtaining access to the WAN/LAN and OMS II.

Failing to properly grant access to users could allow for an increased risk of the system being compromised by unauthorized individuals. Further, unauthorized user account access may result in the loss of data, data corruption, and/or other privileged access.

We recommend that Mint management:

1. Implemented an oversight process to ensure that Mint personnel are complying with Mint account management policies and procedures.
2. Validate that the existing WAN/LAN and OMS II user accounts are still appropriate.

Management Response:

Management concurs with the finding.

A-2 Controls over Timely Removal of Inactive Users from the Mint Network Should be Strengthened

Three WAN/LAN user accounts had gone unused for more than 90 days and were not disabled as required by Mint policy.

Mint Wiki *Network Account Disabling and Removal Procedures,* states:

> Employees:
>
> The ITD Service Desk must disable a government employee's account upon notification that the employee has departed the United States Mint or when the account has been inactive for 90 consecutive days (in both AD and RSA console). After 90 days of being disabled, the account must be archived. After 90 days of being archived, the account and all associated files must be removed from the network.

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:
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

Due to lack of management's oversight of unused accounts, Mint was unaware that it needed to remove the user accounts that were inactive for over 90 days.

To the extent that valid inactive accounts are present in WAN/LAN, these user accounts have an increased risk of being compromised by unauthorized individuals and, therefore, of being used to access, disclose, and/or modify production data.

We recommend that Mint management:

1. Configure the WAN/LAN to disable user accounts automatically after 90 days of inactivity.
2. Validate that the existing three WAN/LAN user accounts are still appropriate.

Management Response:

Management concurs with the finding.

A-3 Controls over Mint's WebTA User Access Review and Recertification Should be Strengthened

Fiscal Service Administrative Resource Center (ARC) is responsible for administering Mint's instance of Web Time and Attendance (WebTA). On an annual basis, ARC provides Mint with listing of existing WebTA users and their privileges and requests that Mint notify ARC of any need access adjustments.

The Mint Philadelphia office did not complete and submit its review and recertification of its WebTA users. As a result, Mint was unware if the existing Philadelphia office users' accounts and privileges were still appropriate and could not subsequently notify ARC of any needed access adjustments.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2, 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];
>
> g. Monitors the use of information system accounts
>
> h. Notifies account managers;
>
> 1. When accounts are no longer required
>
> 2. When users are terminated or transferred;
>
> 3. When individual information system usage or need-to-know changes;
>
> i. Authorizes access to the information system based on:
>
> 1. A valid access authorization;
>
> 2. Intended system usage; and
>
> 3. Other attributes as required by the organization or associated missions/business functions;
>
> j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency];

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Due to a lack of written policies, Mint offices and sites are not consistently following the WebTA account review and recertification process.

Failing to review employee access and privileges in WebTA annually and to remove or modify accounts as needed can allow for unauthorized access and modification of production data.

We recommend that Mint management:

1. Develop formal procedures for completing and submitting the annual WebTA user access review and recertification.
2. Evaluate the WebTA users defined to the Philadelphia site and ensure that the current user access and privileges are still appropriate.

Management Response:

Management concurs with the finding.

A-4 Controls over Terminated Individual's HR Connect Access Should be Strengthened

HR Connect is an enterprise-wide human resources management system owned and administered by the Department of Treasury (Treasury). Treasury's HR Connect Program Office (HRCPO) is the Bureau of the Fiscal Service Administrative Resource Center's (ARC's) partner as a designated shared service center through the HR Line of Business. HR Connect allows managers to electronically initiate, approve, track personnel actions, awards, and performance appraisals, and view a variety of personnel data on employees reporting to them or their supervisors. Employees can review and request changes to their own personnel information. HR Connect is a front-end system for sending personnel action data to the USDA National Finance Center's Payroll/Personnel System.

One of 119 terminated Mint users still had active access to the HR Connect system and had retained active access for 2 months and 19 days since his/her termination. Although the user did not have privileged access, the risk exists that the account could have been accessed by the former employee, or other nefarious party, to aid in the fraudulent disbursement of payroll and/or other benefits.

Mint Minimum Standard Parameters, March 20, 2017, states:

6.1.4 Delete Users

Bureau of the Fiscal Services, Administrative Resource Center provides account management services for HR Connect.

6.1.5 Remove Inactive Users

The United States Mint, Workforce Solutions Department points of contact for HR Connect receives a listing from the Bureau of the Fiscal Services, Administrative Resource Center annually to review and validate United States Mint personnel authorized to access HR Connect; this will include a list of all United States Mint users to review and validate that only current United States Mint users are in the system; and provide a response back to the Bureau of the Fiscal Services point of contact for HR Connect to disable accounts for United States Mint users that no longer require access to HR Connect based on the change of current job functions or departure from the United States Mint. United States Mint Workforce Solutions Department will request an updated listing though the OracleSupportTeam@fiscal.treasury.gov to validate changes. The frequency of the reviews and validations may change from annually to quarterly to ensure timely changes

and to align with Treasury Directive 85-01 and United States Mint access policy to facilitate the removal of users who have been inactive for 90 or more days.

Treasury Directive Publication 85-01*, Department of the Treasury Information Technology Security Program,* July 1, 2016, states,

Section 2.9 System Owner (SO)

For each information system under their purview, SOs shall –

3) Grant access to the system with associated rights and privileges, giving individuals the fewest possible privileges necessary for job performance so that privileges are based on a legitimate need. Further, re-evaluate access privileges periodically (at least annually) and revoke access in a timely manner upon personnel transfer or termination

Mint management does not have a requirement, documented in a policy and procedure, specifying the timeframe within which to notify ARC to disable or delete the account of a terminated individual.

Failing to disable terminated users accounts timely could allow for an increased risk of the system being compromised by unauthorized individuals. Further, unauthorized user account access may result in the loss of data, data corruption, and/or other privileged access.

We recommend that Mint management:

1. Update Mint HR Connect policies and procedures to specify the period to remove the access of terminated users from the HR Connect system.
2. Remove terminated user access in accordance with recommendation 1.

Management Response:

Management concurs with the finding.

Appendix B

THE UNITED STATES MINT

Status of Prior Year Management Letter Comments

Fiscal Year 2016 Management Letter Comments	Fiscal Year 2017 Status
General IT Controls	
A-1 Controls over User Account Management Should be Strengthened	Re-issued, A-1
A-2 Controls over HR Connect Periodic User Access Review Should be Strengthened	Closed
A-3 Controls over HR Connect Third Party Applications Security Controls Monitoring Should be Strengthened	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