Audit Report

OIG-17-030

FINANCIAL MANAGEMENT

Management Letter for the Audit of the United States Mint's Fiscal Years 2016 and 2015 Financial Statements

December 21, 2016

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 21, 2016

**MEMORANDUM FOR RHETT JEPPSON, PRINCIPAL 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 2016 and 2015 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, 2016 and 2015, 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. 15-02, *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 9, 2016, that discusses certain matters involving internal control over financial reporting 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

THIS PAGE INTENTIONALLY LEFT BLANK

THE UNITED STATES MINT

MANAGEMENT LETTER

FOR THE YEAR ENDED SEPTEMBER 30, 2016

THE UNITED STATES MINT
MANAGEMENT LETTER

FOR THE YEAR ENDED SEPTEMBER 30, 2016

TABLE OF CONTENTS

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

December 9, 2016

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

Principal 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, 2016 and 2015, 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. 15-02, *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.

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 our testwork we noted that controls over user account management were not operating effectively. Specifically we noted the following:

- One (1) of 15 Wide Area Network (WAN)/Local Area Network (LAN) user accounts was created prior to access being properly approved.
- One (1) of 7 Order Management System (OMS) II users was not properly approved prior to being granted access. The user requested access for himself, and additional manager or supervisor approval was not obtained.

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.

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.

Treasury Directive Publication (TD P) 85-01, Version 2.4.3, 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

The Mint management indicated that the WAN LAN user account was created when the employee started at the Mint, but not authorized until the employee returned from a 13 week training course for new officers. Additionally, for the OMS II user account, Mint management did not require supervisor's approval before OMS II access is granted to a manager.

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. Improve an enforcement mechanism to ensure that new users are approved in accordance with TDP 85-01 when granting them access to the WAN/LAN and OMS II.
2. Require supervisor's approval before granting user access to a manager.

Management Response:

Management concurs with the finding.

A-2 Controls over HR Connect Periodic User Access Review Should be Strengthened

The Mint utilizes the HR Connect application to process their personnel and payroll transactions. The HR Connect application is managed by the Treasury Enterprise Business Services, and the application and its general support system (GSS) is hosted by the Treasury Departmental Offices (DO). Since no Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report or other attestation report was available, we tested relevant general IT controls (GITCs) at Treasury's Enterprise Business Services and DO in support of the FY 2016 Mint financial statement audit.

During our testwork we noted that Mint management did not perform an annual review of its privileged HR Connect user accounts, as required by the Mint Information Systems Access Policy and NIST SP 800-53.

The Mint Information System Access Policy, Dated August 2015, states:

> Workforce Solutions Department (WSD): will receive from the Bureau of Fiscal Services (BFS) Administrative Resource Center (ARC) annually: 1) a list of all United States Mint users to review and validate that only current United States Mint users are in the system and that assigned permissions represent current job functions and 2) BFS/ARC Internal HR Connect HR Roles, BFS/ARC users with Mint HR Connect roles, and current policies and procedures for Annual Recertification for HR Connect for United States Mint WSD and Information Security Division to review and validate access control procedures are compliant.

National Institute of Standards and Technology SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CM-7, states:

> The organization:
>
> a. Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and
>
> b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

The Mint Management did not complete the review of its privileged HR Connect user accounts due to competing priorities and lack of resources.

Failing to properly reauthorize 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. Develop and implement policy and procedures to review the access of privileged Mint HR Connect users on a defined frequency.
2. Review the access of privileged HR Connect users based on the frequency defined in procedures mentioned in Recommendation No. 1.

Management Response:

Management concurs with the finding.

A-3 Controls over HR Connect Third Party Applications Security Controls Monitoring Should be Strengthened

The Mint utilizes the HR Connect application to process their personnel and payroll transactions. The HR Connect application is managed by the Treasury Enterprise Business Services, and the application and its general support system (GSS) is hosted by the Treasury Departmental Offices (DO). Since no SSAE 16 report or other attestation report was available, we tested relevant GITCs at Treasury's Enterprise Business Services and DO in support of the FY 2016 Mint financial statement audit.

In prior years, Mint management assessed the effectiveness of HR Connect's security controls performed at Treasury Enterprise Business Services and DO. However, in FY 2016, Mint management did not assess the effectiveness of the HR Connect security controls, which does not comply with Treasury Directive Publication (TD P) 85-01 and National Institute of Standards and Technology (NIST) 800-53.

TD P 85-01, Version 2.4.3, Control AC-20, states:

> The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
>
> a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
>
> b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-20, states:

> The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
>
> a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
>
> b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
>
> Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

The Mint Management did not complete the review of HR Connect controls due to competing priorities and lack of resources.

Without adequate third party oversight, Mint is unable to ensure their IT security policies and procedures are being enforced. Mint cannot provide a basis by which management can ensure security measures are working, and the exposure for unauthorized access to data is increased. This exposure could result in potential data breach, increased errors, inadvertent deletion of data, and/or critical management decisions based on incorrect, invalid, or inconsistent data.

We recommend that Mint management:

1. Develop and implement policy and procedures to assess the key HR Connect security controls managed by Treasury Enterprise Business Services and DO on a defined frequency.
2. Assess the effectiveness of the HR Connect security controls based on the frequency determined from recommendation No. 1. For any control gaps identified by Mint management, assess mitigating controls if applicable.

Management Response:

Management concurs with the finding.

Appendix B

THE UNITED STATES MINT

Status of Prior Year Management Letter Comments

Fiscal Year 2015 Management Letter Comments	Fiscal Year 2016 Status
Financial Resources	
A-1 Controls over the Review of Service Providers Reports Should be Strengthened	Closed
Inventory Management	
B-1 Controls over the San Francisco Cycle Count Should be Strengthened	Closed
General IT Controls	
C-1 Controls over the Review of Terminated Users Should be Strengthened	Closed

THIS PAGE INTENTIONALLY LEFT BLANK

Treasury OIG Website

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

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx