UNITED STATES CAPITOL POLICE

OFFICE OF INSPECTOR GENERAL

Fiscal Year 2016 Management Letter

Report Number OIG-2017-03

December 2016

~~*Report Restriction Language*~~

INSPECTOR GENERAL

To: Matthew R. Verderosa,
Chief of Police

From: Fay F. Ropella, CPA, CFE
Inspector General

Subject: Management Letter Related to the Audit of the United States Capitol Police Fiscal Year 2016 Financial Statements (Report No. OIG-2017-02)

In planning and performing our audit of the financial statements of the United States Capitol Police (USCP or the Department) as of and for the year ended September 30, 2016 (FY 2016), in accordance with auditing standards generally accepted in the United States of America, we considered USCP'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 opinions on the financial statements and on internal control over financial reporting.

We previously issued our opinions on USCP financial statements and internal control over financial reporting as of September 30, 2016 in our Independent Auditors' Report dated December 2, 2016, (Report No. OIG-2017-02), in which we communicated the material weaknesses and significant deficiency. However, during our audit we became aware of control deficiencies other than the material weakness and significant deficiency which provide opportunities to strengthen USCP internal controls and improve the efficiency of your operations. This communication does not affect our Independent Auditors' Report, dated December 2, 2016.

While the nature and magnitude of these other deficiencies in internal control were not considered important enough to merit the attention of those charged with governance, they are considered of sufficient importance to merit management's attention. We have summarized the FY 2016 management letter comments and recommendations and USCP responses, and present the FY 2016 status of FY 2015 management letter comments in Section III.

USCP management and governance are the sole intended users of this information and we do not intend for its use by anyone other than these specified parties.

United States Capitol Police
FY 2016 Management Letter

Table of Contents

I. Introduction

We provided USCP management a Notice of Findings and Recommendations (NFR) matrix with 13 findings related to the fiscal year (FY) 2016 financial statements audit. A finding is a written communication to management of an issue identified during the audit. We categorized a finding or a combination of findings as a material weakness (MW), a significant deficiency (SD), or a management letter comment (MLC). We have included findings categorized as MW or SD in our separate report titled Independent Auditors' Report on Internal Control over Financial Reporting dated December 2, 2016. We categorized three of the 13 findings in the NFR matrix as MWs, one as SD, and nine as MLCs (see Section II).

We also included FY 2016 status of our FY 2015 MLCs in section III.

II. Management Letter Comments

MLC 1: [redacted] Database Change Control Segregation of Duties Issues (Modified Repeat Comment[1])

In the prior year, the Office of Information Systems (OIS) had two accounts with administrator level access to both development code repository and [redacted] production databases. During 2016, management changed account privileges for the two accounts in both production and development, removing administrative access to one account in production. However, the two users have a shared administrator account to transfer code changes into the production [redacted] environment.

USCP also was not independently monitoring the database and operating system activity of these accounts to mitigate the potential segregation of duties risk. Management indicated that they plan to include database monitoring in the agency Security Information and Event Management (SIEM) Solution. During FY 2016, OIS created tracking of event logs for [redacted] production and development servers. However, the SIEM, which aggregates the log files, did not have the ability to show detailed review of user activity.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*, control AC-5 which states, "the organization: separates [Assignment: organization-defined duties of individuals]; documents separation of duties of individuals; and defines information system access authorizations to support separation of duties."

[1] During FY 2015, the auditor noted this finding as part of a Material Weakness related to payroll processing in the Independent Auditor's Report. During FY 2016, we downgraded this issue to a Management Letter Comment. Therefore, this is a repeat finding, but it did not appear on the FY 2015 Management Letter.

Recommendation 1: We recommend that the United States Capitol Police Office of Information Systems implement mitigating controls to review logs and be alerted of suspicious activities surrounding [redacted] development.

Management Response:

Concur: OIS plans to implement a more advanced SIEM to allow automated monitoring and alerting of privileged accounts during FY 2017, pending funding.

MLC 2: Current Authorizations to Operate were not Documented (Modified Repeat Comment)

In the prior year, USCP was transitioning to continuous monitoring and authorization as prescribed by NIST SP 800-37 Revision 1 to replace the cycle of 3-year certification and accreditation. As of FY 2016, USCP had not fully implemented NIST SP 800-37 Revision 1. USCP currently operated on a one-third control review annually; however, USCP only performed an assessment of common controls during FY 2016.

For FY 2016, Infrastructure and [redacted] Systems did not have documented authorizations to operate as required by USCP's risk management framework (RMF) process. The infrastructure general support system did not have a current system security plan, risk assessment, or recent security assessment report. The [redacted] major application had a system security plan, risk assessment, and security assessment report; however, OIS did not formally authorize the system to operate.

USCP management had issued a Security Accreditation Package memorandum in December 2014, indicating that all systems were in continuous monitoring phase for the agency's RMF. The Memorandum also indicated that if the risk were deemed acceptable all Office of the Chief Information Officer systems would be available for Designated Approval Authority in 2015. The memorandum also noted that USCP monitors and continuously assesses security risks through methods including ongoing change management and vulnerability assessments. However, OIS indicated in a follow-up memorandum dated August 28, 2015 that they were realigning the systems.

OIS scheduled the authorization process for the infrastructure general support system to begin in November 2015. However, the infrastructure system had not completed security control testing and updated documentation in pursuit of the realignment during the fiscal year.

USCP RMF Process and NIST SP 800-37 revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* requires that agencies prepare authorization packages for major systems and have them authorized by an authorizing official as part of a continuous monitoring process.

Recommendation 2: We recommend that the United States Capitol Police (USCP) Office of Information Systems ensure the General Support and [redacted] systems receive authorizations to operate in line with USCP policies and procedures.

Recommendation 3: We also recommend that the United States Capitol Police Office of Information Systems document system security plans, risk assessments, and security assessment reports for the General Support System and [redacted] supporting authorization operating decisions.

Management Response:

Concur: OIS plans to review current authorizations to operate and realign into compliance with NIST 800-53 Rev. 4, which includes, but not limited to, continuous monitoring, risk assessments, vulnerability assessments and remediation, and incident management.

MLC 3: [redacted] Version is not Supported by the Vendor (Modified Repeat Comment)

During FY 2015, the auditor noted that USCP no longer had vendor support for its asset management application, [redacted]

The inter-agency agreement between USCP and the Library of Congress (LOC) indicated that LOC Application Management Services was responsible to "Monitor security patches and updates from the software vendor(s) and recommending patches to apply." The agreement goes on to state: "The USCP will: Maintain appropriate licenses and maintenance agreements with the applicable software vendors." Since the manufacturer no longer supports the version of [redacted] the vendor will no longer provide additional patches.

USCP was receiving support through LOC and [redacted] As previously stated, USCP was responsible for all licensing and maintenance agreements of [redacted] from the vendor and the version of [redacted] used by USCP, which remained unsupported for FY 2016.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control SI-2 states the following, "the Organization: Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates."

Recommendation 4: We recommend that the United States Capitol Police Office of Information Systems upgrade the [redacted] application to a vendor supported version.

Management Response:

Concur: OIS is currently working with the vendor [redacted] to upgrade the [redacted] solution to the latest (supported) version of software and is expected to be running on the supported software this coming summer.

MLC 4: Unsupported Microsoft Operating Systems (Modified Repeat Comment)

USCP was operating three Windows Server 2003 systems, which Microsoft dropped from extended support as of July 14, 2015. These servers support the [redacted] application. USCP was also running one Windows XP system that Microsoft dropped from extended support as of April 8, 2014. Once Microsoft's extended support phase ends security updates will no longer be released. Management indicated that they plan to replace the 2003 devices once they upgrade [redacted] in the production environment to version 6.2. We notified management of the one Windows XP system, and they removed it from the network.

According to NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control SI-2 , "the organization: Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates." However, no further security updates are available for unsupported software.

Recommendation 5: We recommend that the United States Capitol Police Office of Information Systems upgrade the [redacted] server's operating systems to supported versions.

Management Response:

Concur: OIS is in the process of upgrading [redacted] and once the upgraded version is released later this year these servers will be decommissioned.

MLC 5: Policies and Procedures not Approved and Communicated Across the Organization (New Comment)

USCP utilizes policies and procedures for operations. In certain cases, OIS has not completed its formal approval processes and policies. In certain instances, the draft policies included instructions for individuals outside of OIS. For example, we noted the [redacted] draft policy had a section stating, "Heads of Bureaus and Offices are responsible for..." Without an officially approved policy, individuals outside of OIS may be unaware of their responsibilities under draft policies and the Department cannot hold employees accountable for noncompliance with draft policies.

The following is a listing of unapproved policies: [redacted]

[redacted]

At the end of our fieldwork, the Office of Financial Management (OFM) was in the process of updating the [redacted] Security Policy and Configuration.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Controls PM-1 states, "the organization: develops and disseminates an organization-wide information security program plan that: Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation."

Recommendation 6: We recommend that the United States Capitol Police Office of Information Systems in cooperation with the Office of Financial Management formally document and approve information security policies and distribute the policies to responsible bureaus and offices.

Management Response:

Concur: OIS plans to review, update, and/or create necessary policies and procedures during FY 2017 to ensure all policies and procedures are current, align with best practice, reviewed annually, updated as needed, and distributed to the necessary parties.

MLC 6: Security Awareness Training not Completed in a Timely Manner (New Comment)

USCP employees did not complete security awareness training in a timely manner. Specifically, 2 of 16 new hires had not completed the required Security Awareness Training as part of their on-boarding process. In addition, two had not signed the required OIS [redacted], which is included with the online security awareness training.

Furthermore, one of four sampled [redacted] users had not taken the required Security Awareness Training.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control AT-2 states, "the organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): as

part of initial training for new users; when required by information system changes; and [Assignment: organization-defined frequency] thereafter."

In addition, OIS's [redacted] requires new personnel and contractors to complete the Security Awareness Training and Privacy Awareness Training within seventy-two hours of the creation of a network account.

Recommendation 7: We recommend that the United States Capitol Police Office of Information Systems implement a process to ensure all personnel and contractors receive security awareness training within agency-required timeframes.

Management Response:

Concur: OIS plans to implement a system that integrates with Active Directory (AD) to ensure accounts are disabled until security awareness training is complete prior to account activation. Furthermore, to have automated reports alerting of any employee/contractor that have not completed the training within the policy timeline.

MLC 7: Monitoring of User Entity Controls for [redacted] (New Comment)

[redacted] host USCP's [redacted] and [redacted] applications in their [redacted] Data Center. USCP maintained a direct Virtual Private Network connection with [redacted] to facilitate application access. It is the responsibility of USCP to ensure that the environment and connection between both [redacted] and USCP are secure. [redacted] maintained an independent *Statement on Standards for Attestation Engagements* (SSAE) 16 audit of the [redacted] Data Center, which includes potential weaknesses and user entity controls that USCP would need to implement to rely on the [redacted] environment. However, neither OIS nor OFM reviewed the SSAE 16 user entity controls.

According to NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control AC-20 "the organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: access the information system from external information systems; and process, store, or transmit organization-controlled information using external information systems."

Recommendation 8: We recommend that the United States Capitol Police Office of Information Systems document and implement a procedure for reviewing third party Statements on Standards for Attestation Engagement 16 reports and implement applicable controls.

Management Response:

Concur: OIS plans to review, update, and/or create necessary policies and procedures during FY 2017 to ensure all policies and procedures are current, align with best practice, reviewed annually, updated as needed, and distributed to the necessary parties.

MLC 8: Purchase Cards – Certification Report Forms not Signed by the Approving Official (New Comment)

Purchase cardholders did not always sign purchase card certification forms in a timely manner, indicating untimely completion of the certification report form. Additionally, 3 of 15 purchase cardholder-approving officials did not sign the Certification Report Form. Seven purchase cardholder did not accurately reconcile the Citibank statement to their purchase log.

USCP Standard Operating Procedure [redacted], Dated August 22, 2011, stated,

1) The Approving Official (AO) ensures that Purchase Card transactions for the assigned Card Holders are legal, proper, and correct in accordance with governing rules and regulations.
2) The AO obtains and prints a consolidated monthly report from the Citibank website detailing all transactions for each of the AO's assigned Card Holders during the designated billing period. The AO uses this report to complete the review of each Card Holder Statement of Account as follows:
    a) Reconciles the consolidated monthly report with individual Statements of Account received from each Card Holder.
    b) Verifies that all purchases were properly approved and that supplies or services were received on time and in the quantity/quality ordered.
    c) Verifies that all transactions were valid and that all purchases were made in accordance with the USCP Purchase Card Program policy.
    d) Ensures that the Card Holder Dispute Forms for all disputed transactions were properly completed and forwarded to Citibank and to the Agency/Organization Program Coordinator.
    e) Resolves outstanding questions and verifies, certifies, and signs each USCP Purchase Card Holder and Approving Official Certification Report Form.

Recommendation 9: We recommend the United States Capitol Police (USCP) design controls to enforce its purchase card policy, which requires approving officials to sign the Purchase Cardholder/Approving Official Certification Report Form. Additionally we recommend USCP design controls to enforce its purchase card policy, which requires the cardholder to complete the Purchase Cardholder/Approving Official Certification Report Form in a timely manner.

Management Response:

USCP will hold various training sessions with Cardholders and Approving Officials to provide refresher training on the responsibilities for signing the Approving Official Certification Form and the timeliness of submitting the Approving Official Certification Form(s) to the Approving Official. USCP will also conduct spot quarterly reviews using a sample process to ensure compliance with its policies.

MLC 9: Annual Performance Reports – Not Completed and Returned to the Office of Human Resources (OHR) (New Comment)

The Office of Inspector General selected a sample of 45 employees for internal control payroll testing. Our sample consisted of 15 newly hired employees, 15 separated employees, and 15 existing employees. Of the 15 existing employees, 10 did not have an annual performance evaluation in their personnel file kept by OHR newer than July 2015. Our review of these files took place in October of 2016.

The Commission on Accreditation for Law Enforcement Agencies *Standards for Law Enforcement Agencies* Chapter 35.1.2 states, "A written directive requires a performance evaluation of each full-time employee and reserve officer be conducted and documented at least annually with the exception of the agency CEO, constitutionally elected officials, or those employees exempted by controlling legislation."

Furthermore, USCP Directive [redacted] Dated May 28, 2012, states, "Annual performance planning by the supervisor and employee, a midyear performance review, and ongoing monitoring, assistance, and coaching."

The directive additionally states, "The employee's original PECS Performance Planning and Appraisal Form (Closeout or Rating of Record) will be retained in the employee's Central Personnel File in OHR for three years and a copy will be maintained in the employee's Unit Personnel File for one year."

Recommendation 10: We recommend that the United States Capitol Police design a control to ensure compliance with its [redacted] policy, which requires completion of a performance evaluation for each employee on an annual basis. Additionally, we recommend that management provide all performance reports to the Office of Human Resources in a timely manner and file in personnel folders.

Management Response:

OHR currently is assessing its performance management program to address issues such as this. The end result will be increased training for supervisors on how to conduct meaningful performance appraisals, hold supervisors accountable through their own appraisal reviews for timely completion of performance plans and appraisals, and ties between performance appraisals

and awards and other recognition. The combined effect will be to increase adherence to USCP policy on conducting performance reviews with a goal of 100% compliance.

OHR also is assessing the National Finance Center's Performance module which will allow for the creation of performance plans and appraisals electronically and which will allow for simple retrieval for inclusion in an employee's Central Personnel File.

III. FY 2016 Status of Prior Year (FY 2015) Management Letter Comments

USCP's FY 2015 management letter identified four management letter comments. We closed one of the MLCs and modified three repeat comments as shown below.

FY 2015 Comment No.	Comment	FY 2016 Status
1	Travel Voucher Payments	Closed
2	Current Authorizations to Operate were not Documented	Modified Repeat Comment. See MLC 2.
3	[redacted] Version is not Supported by the Vendor	Modified Repeat Comment. See MLC 3.
4	Unsupported Microsoft Operating Systems	Modified Repeat Comment. See MLC 4.

CONTACTING THE OFFICE OF INSPECTOR GENERAL

Success of the OIG mission to prevent fraud, waste, abuse, or mismanagement depends on the cooperation of employees and the public. There are several ways to report questionable activity.

Call us at 202-593-3868 or toll-free at 866-906-2446. A confidential or anonymous message can be left 24 hours a day/7 days a week.

Toll-Free
1-866-906-2446

Write us:
United States Capitol Police
Attn: Office of Inspector General
499 South Capitol St. SW, Suite 345
Washington, DC 20510

Or visit us:
499 South Capitol Street, SW, Suite 345
Washington, DC 20003

You can also contact us by email at: OIG@USCP.GOV

When making a report, convey as much information as possible such as:
Who? What? Where? When? Why? Complaints may be made anonymously or you may request confidentiality.

Additional Information and Copies:

To obtain additional copies of this report, call OIG at 202-593-4201.

OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL