UNITED STATES CAPITOL POLICE

OFFICE OF INSPECTOR GENERAL

Management Letter
Related to the Audit of the United States Capitol Police's Fiscal Years 2017 and 2016 Financial Statements

Report Number OIG-2018-05

December 2017

Report Restriction Language

~~**Distribution of this Document is Restricted**~~

~~This report may contain sensitive law enforcement information and/or is part of the deliberative process privilege. This is the property of the Office of Inspector General and is intended solely for the official use of the United States Capitol Police, the Capitol Police Board, or any agency or organization receiving the report directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the United States Capitol Police or Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20510

INSPECTOR GENERAL

December 15, 2017

MEMORANDUM

TO: Matthew R. Verderosa
Chief of Police

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

SUBJECT: *Management Letter* (Report No. OIG-2018-05) *Related to the Audit of the United States Capitol Police's Fiscal Year 2017 Financial Statements* (Report No. OIG-2018-04)

We have attached the subject report for your review and action. This management letter discusses a number of internal control deficiencies identified during the audit of the financial statements. The Office of Inspector General (OIG) considers these control deficiencies important enough to merit management's attention, and if addressed, could enhance the efficiency and effectiveness of internal controls.

These deficiencies, although of concern, did not rise to the level necessary to be included in the report on the financial statement audit. OIG included your comments related to the Notice of Findings and Recommendations (NFRs) Department management indicated that it did not have any additional comments beyond those that they provided on NFRs matrix during the audit. Therefore, we have incorporated management responses received in the NFRs matrix in the management letter.

Since we made and reported these comments in a management letter rather than within a material weakness or significant deficiency framework, OIG will not track these recommendations through our formal compliance process. However, we will evaluate compliance during our future audits of the Department financial statements.

I would like to express my appreciation for the cooperation and assistance provided by the Department during this effort. If you have any questions regarding this report, please contact me on [redacted] or have your staff contact [redacted]

Attachment: As stated.

cc: Assistant Chief Steven Sund, Chief of Operations
Mr. Richard Braddock, Chief Administrative Officer
[redacted] Audit Liaison (5 copies)

499 South Capitol Street, SW, Washington, DC 20003 202-593-4555

Management Letter
Related to the Audit of the
United States Capitol Police's
Fiscal Years 2017 and 2016 Financial Statements

TABLE OF CONTENTS

Introduction

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, 2017 and 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.

The Office of Inspector General (OIG) previously issued our opinions on USCP financial statements and internal control over financial reporting as of September 30, 2017 in our *Independent Auditor's Report* dated December 6, 2017, (Report No. OIG-2018-04), in which we communicated a material weakness related to payroll controls. However, during our audit the OIG became aware of control deficiencies other than the material weakness, which provide opportunities to strengthen USCP internal controls and improve the efficiency of your operations. This communication does not affect our *Independent Auditor's Report*, dated December 6, 2017.

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.

OIG provided USCP management a Notice of Findings and Recommendations (NFR) matrix with 10 findings related to the Fiscal Year (FY) 2017 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[1]). We have included findings categorized as MW or SD in our separate report titled *Independent Auditor's Report on Internal Control over Financial Reporting* dated December 6, 2017. We categorized 3 of 10 findings in the NFR matrix as MWs, and seven as MLCs. USCP's *Fiscal Year 2016 Management Letter* (Report No. OIG-2017-03) identified nine management letter comments. We closed four of the previously reported MLCs, modified two and repeated three comments. OIG made two new findings during FY 2017 financial statement audit.

[1] *Fiscal Year 2016 Management Letter* (Report Number OIG-2017-03.)

Management Letter Comments

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

In 2016, the Office of Information Systems (OIS) had two accounts with administrator level access to both development code repository and [redacted] production databases. During 2017, OIS 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 [redacted]

The 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 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."

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.

Status of Recommendation: Repeat Finding. Some Progress.

Management Response: Concur. [redacted]

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

The Department was continuing their transition to continuous monitoring and authorization as prescribed by NIST, SP 800-37 Revision 1. As of September 30, 2017, USCP had not fully

implemented NIST SP 800-37 Revision 1.

During FY 2017, USCP restructured the WAN/LAN/PoliceNet system into the [redacted] and conducted a major application upgrade to the [redacted] time and attendance system. OIS did not complete the security authorization packages including the authorizations to operate and supporting system security plans and security assessment reports after the major changes. The auditors could not fully assess the [redacted] and [redacted] security management functions.

USCP Risk Management Framework 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 Office of Information Systems ensure the [redacted] and [redacted] systems receive authorizations to operate in line with United States Capitol Police 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 [redacted] and [redacted] supporting authorization operating decisions.

Status of Recommendation 2 and 3: Modified Repeat Finding. Limited Progress.

Management Response: Concur. As of November 15, 2017, majority of the [redacted] documents have been created and signed. The enterprise list of applications is under review and being categorized accordingly. All documents for the [redacted] ATO[2] have been created and signed; however, since this is a "major application" there are several controls under the [redacted] which need completion before the [redacted] ATO can be issued. Both ATOs are in progress.

MLC 3: Monitoring of User Entity Controls (Repeat Comment)

[redacted]

[2] ATO – Authority to Operate.

[redacted]

[redacted]

Recommendation 4: We recommend that the United States Capitol Police Office of Information Systems, document and implement a procedure for reviewing third party Statement on Standards for Attestation Engagements 18 audit reports and implement applicable controls.

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Concur. The [redacted] The OIS Cyber team reviewed the report to ensure the complementary user controls are in place and compliant. Additionally, the Chief Information Security Officer has been added to the contact list to ensure updates to the SSAE are sent to USCP.

MLC 4: Purchase Cards – Approving Official Did Not Sign Certification Report Forms (Modified Repeat Comment)

Overall, the Department did not adequately design internal controls and processes in a way that would ensure successful implementation and administration over its Purchase Card Program. The Department's purchase card guidance was outdated and inconsistent and did not provide sufficient monitoring and oversight for compliance. Controls were not sufficient and did not ensure that cardholders recorded the correct budget-object-classification codes. As a result, numerous non-compliance issues were brought to light.

Recommendation 5: We recommend the United States Capitol Police 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 the United States Capitol Police design controls to enforce its purchase card policy, which requires the cardholder to complete the Purchase Cardholder/Approving Official Certification Report Forms in a timely manner. The Office of Procurement must comply with Department Guidance requiring an Annual Purchase Card Program Review.

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Concur. The Department is working aggressively to resolve all audit findings related to the Purchase Card program during the first quarter of FY 2018 and expects no further issues in future financial statement audits.

MLC 5: Annual Performance Reports – Department Supervisors Did Not Complete or Return Annual Performance Reports to the Office of Human Resources (OHR) (Repeat Comment)

USCP Directive [redacted], dated May 28, 2012 states, "The employee's original [redacted] 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."

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

We 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, 8 did not have an annual performance evaluation in their personnel file kept by OHR. The most recent performance evaluation was July 2015. We reviewed these files in October 2017.

Recommendation 6: 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.

Status of Recommendation: Modified Repeat Finding. No Progress.

Management Response: Concur. The Department is currently revising policy on both PECS and the Executive Performance Appraisal System and enforcement of the policy will occur in accordance with the revised policy. As a result, all recommendations will be met during FY 2018.

MLC 6: Vulnerability Scanning and Review (New Comment)

USCP's OIS Management changed its vulnerability management scanner from [redacted] to [redacted] during FY 2017. OIS management refocused the patching and remediation process to resolve the top ten patches that would remediate the most vulnerabilities as reported by [redacted]. However, this approach did not address remediation timeframes focused on critical, high, medium, or low. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control RA-5 states, "the organization: Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with

an organizational assessment of risk."

USCP Directive [redacted], dated April 21, 2017 Appendix A, indicates the following for Windows, Linux, and Network equipment "All patches will be applied within 30 days, unless the patch is not applicable to USCP."

Recommendation 7: We recommend that the United States Capitol Police Office of Information Systems, update the vulnerability remediation process and policies to address all vulnerabilities in a specified timeframe or document mitigating controls and acceptance of risk.

Status of Recommendation: New Finding.

Management Response: Concur. OIS implemented a Vulnerability Standard Operating Procedure (SOP) on 27 April 2017, which follows NIST 800 Rev 4 to address the identifying and mitigating vulnerabilities. The required scanning tools and techniques are supported by risk assessments to remediate legitimate vulnerably in accordance with their assessments and response timeframes. Following the SOP for the past 6 months, the OIS Cyber team also implemented (and shown to the OIG) the [redacted] tool that assesses the USCP network on a continual basis to discover, report, and track remediation of discovered vulnerabilities; of which, a tactical plan is in progress to remediate older vulnerabilities and address new vulnerabilities.

MLC 7: Account Separation (New Comment)

From a sample of 10 separated individuals, 1 individual retained account access to the USCP network. The individual had separated on November 30, 2016; however, the account was last accessed on December 16, 2016. The USCP did disable the account after the USCP rule of 90-day inactivity account review. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control AC-2 states, "the organization: Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. Notifies account managers: when accounts are no longer required and when users are terminated or transferred."

Recommendation 8: We recommend the Office of Information Systems review the listing of separated individuals to ensure that all accounts have been disabled on a timely basis.

Status of Recommendation: New Finding.

Management Response: Concur. As of November 15, 2017, all separated employee accounts have been disabled or deleted; as directed by the Account Management Directive. As an additional check on account access and use, the OIS Cyber team receives and reviews a daily [redacted] report for accounts not utilized within 30 days and determines the user's

employee status. Additionally, the OIS Cyber team receives a daily [redacted] report of accounts not utilized (logged in) within 90 days to verify they are disabled and takes action if not. This layered approach provides 3 levels of reviews of account activity to ensure that accounts are only accessible within the allowed timeframes.

FY 2017 Status of Prior Year (FY 2016) Management Letter Comments

OIG reported nine comments in the MLC in FY 2016. We closed four of the MLCs, modified two and repeated three comments as shown below.

FY 2016 Comment No.	Comment	FY 2017 Status
1	[redacted] Database Change Control Segregation of Duties Issues	Repeat. MLC 1.
2	Current Authorizations to Operate were not Documented	Modified Repeat Comment. See MLC 2.
3	[redacted] Version is not Supported by the Vendor	Closed
4	Unsupported Microsoft Operating Systems	Closed
5	Policies and Procedures not Approved and Communicated Across the Organization	Closed
6	Security Awareness Training not Complete in a Timely Manner	Closed
7	Monitoring of User Entity Controls for [redacted]	Modified Repeat Comment. See MLC 3.
8	Purchase Cards – Certification Report Forms not Signed by the Approving Official	Repeat. MLC 4.
9	Annual Performance Report – Not Completed and/or Returned to the Office of Human Resources	Repeat. MLC 5.

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