UNITED STATES CAPITOL POLICE

OFFICE OF INSPECTOR GENERAL

Management Letter
Related to the Audit of the United States Capitol Police's Fiscal Years 2018 and 2017 Financial Statements

Report Number OIG-2019-05

December 2018

~~*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 the 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

December 13, 2018

OFFICE OF INSPECTOR GENERAL

MEMORANDUM

TO: Matthew R. Verderosa
Chief of Police

FROM: Michael A. Bolton
Acting Inspector General

SUBJECT: *Management Letter* (Report No. OIG-2019-05) *Related to the Audit of the United States Capitol Police's Fiscal Year 2018 Financial Statements* (Report No. OIG-2019-04)

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 Thomas Schweinefuss on [redacted]

Attachment: As stated.

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

499 South Capitol Street, SW, Washington, DC 20003 *202-593-4551*

Management Letter
Related to the Audit of the
United States Capitol Police's
Fiscal Years 2018 and 2017 Financial Statements

TABLE OF CONTENTS

	Page
Transmittal Memo	i
Introduction	1
Management Letter Comments	2
[redacted] Database Change Control Segregation of Duties (SOD) Issues (Repeat Comment)	2
Current Authorizations to Operate were not Documented (Repeat Comment)	3
Purchase Cards – Certification Report Forms are not Properly Prepared (Modified Repeat Comment)	3
Performance Reports – Not Completed and Returned to the Office of Human Resources (OHR) (Repeat Comment)	4
Vulnerability Scanning and Review (Repeat Comment)	5
[redacted] (New Comment)	6
FY 2018 Status of Prior Year (FY 2017) Management Letter Comments	8

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, 2018 and 2017, 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, 2018 in our *Independent Auditor's Report* dated December 4, 2018, (Report No. OIG-2019-04), in which we communicated a material weakness (MW) 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 4, 2018.

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 8 findings related to the Fiscal Year (FY) 2018 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 MW, a significant deficiency, or a management letter comment (MLC). We have included findings categorized as MWs in our separate report titled *Independent Auditor's Report on Internal Control over Financial Reporting* dated December 4, 2018. We categorized 2 of 8 findings in the NFR matrix as MWs, and six as MLCs. USCP's *Management Letter Related to the Audit of the United States Capitol Police's Fiscal Years 2017 and 2016 Financial Statements* (Report No. OIG-2018-05) identified seven MLCs. We closed two of the previously reported MLCs, modified one and repeated four comments. OIG made one new finding during FY 2018 financial statement audit.

Management Letter Comments

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

In the prior year, USCP upgraded the [redacted] application. However, roles within the development code repository were not effectively segregated to restrict individuals from transferring the application code from development into production. It was noted that two individuals had the capability to transfer code from the [redacted] development code repository into the production database while maintaining administrative capabilities in the production application. This issue remains unchanged for FY 2018.

During FY 2018, the two user's administrative capabilities were restricted; however, they were capable of proxying to a shared administrative account. The proxying and actions in the production application are logged; however, the logs were not monitored independently.

USCP was not independently monitoring the database and application activity of these accounts to mitigate the potential SOD risk. Management indicated that they plan [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 Organizations*, 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]

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Concur. Development of a SOD matrix across OIS systems is underway with an expected completion within FY19. This matrix will identify potential SOD conflicts within the various systems, applications and environments. Each conflict will be reviewed and mitigated to the fullest extent; Chief Information Officer approval will be required for any risk based decision.

The USCP does forward system event logs, including certain application and database activities. The USCP is actively working on incorporating additional logging capabilities from within databases and applications to further detail identity and authentication activity,

privileged access and any log tampering. These additional capabilities will be incorporated into the SIEM within the next 45 days.

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

USCP was continuing their transition to continuous monitoring and authorization as prescribed by NIST SP 800-37 revision 1. As of September 30, 2018, 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. During FY 2018, OIS was not in compliance with USCP Directive [redacted] dated April 26, 2017, steps 4. Assess and 5. Authorize. OIS did not complete the security authorization packages including the authorizations to operate, supporting system security plans and security assessment reports for FY 2018. Therefore, the auditors could not fully assess the [redacted] and [redacted] security management functions.

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: Repeat Finding. Limited Progress.

Management Response: Concur. In FY 2018, OIS placed a contract for the development and completion of 4 Authorities to Operate with completion dates of FY19Q4. The activities are underway and include accreditation boundaries of both [redacted] and [redacted]

MLC 3: Purchase Cards – Certification Report Forms are not Properly Prepared (Modified Repeat Comment)

Department internal controls that ensure successful implementation and administration over its Purchase Card Program need continued oversight. The Department updated purchase card

directives and standard operating procedures during FY18, the effects of those changes could have only influenced the final months of the year.

A sample of 20 credit card payments (CCP) were tested as part of the FY 2018 financial statement audit. Multiple internal control exceptions were noted. Three cardholders did not sign and date the *Purchase Card Holder/Approving Official Certification Report Form* (Certification Report Form) within the 7 day required period, indicating untimely completion of the reconciliation of the *Purchase Card Buying Log* (Purchase Log) and Citibank statement. One purchase cardholder did not date the Certification Report Form, circumventing the control. Eleven purchase cardholder-approving officials did not properly approve the Certification Report Form. Nine of those officials did not meet the 2 day requirement and 2 of the samples, the purchase cardholder-approving officials did not date their approval of the Certification Report Form.

For 1 of 20 CCP samples, the Citibank statement did not reconcile to the Purchase Log because the cardholder did not follow dispute procedures to correct the vendor erroneously charging the wrong office code that resulted in charging the wrong cardholder.

For 1 of 20 CCP samples, the Purchase Card Buying Log did not reference the correct Credit Card Authorization for one transaction.

Recommendation 4: We recommend the United States Capitol Police continue to rigorously monitor purchase card policy controls to ensure that new policies are effectively implemented.

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Office of Acquisition Management (OAM) will continue its efforts to gain 100% compliance with the requirements of the Purchase Card Program. OAM will ensure that dispute procedures as a part of the reconciliation process are emphasized in the upcoming training to all card holders, as well as the importance of required signatures on all Purchase Card Forms. The training will also include reconciling credits as well.

OAM sends out notifications and reminders for all of the monthly certification packages to all Card Holders and will continue to do so. Additionally, for further accountability measures, the timeliness of the Card Holders and Approving Officials are being tracked monthly via a Purchase Card Compliance Report and the results are being provided, as a part of escalation procedures, to Management for action and compliance.

MLC 4: Performance Reports – Not Completed and Returned to the Office of Human Resources (OHR) (Repeat Comment)

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

OIG 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, 5 did not have an annual performance evaluation in their personnel file kept by OHR. The most recent performance evaluation was April 2015. We reviewed these files in October 2018.

Recommendation 5: 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: Repeat Finding. No Progress.

Management Response: On October 15, 2018, the Department published a revised policy for the PECS program, (Directive [redacted]). The publishing of this Directive closed 3 USCP OIG Audit Recommendations, to include a recommendation that required the Department to demonstrate necessary controls for issuance, completion, monitoring, and documentation ensuring accountability of the appraisal program, were present.

Specifically, the newly published directive includes language under OHR responsibilities that states: Within 60 days of the start of a new appraisal period, and every 30 days thereafter, the OHR will provide a report to Bureau Commanders/ Office Directors of employees within their Bureau/Office who have not yet been placed on a performance plan, until compliance is reached.

Within 60 days of the end of an appraisal period, and every 30 days thereafter, the OHR will provide a report to Bureau Commanders/Office Directors of employees within their Bureau/Office Directors who have yet to receive a final summary rating, until compliance is reached.

The Department believes that substantial progress has been made with this finding and that this recommendation has now been satisfied.

MLC 5: Vulnerability Scanning and Review (Repeat Comment)

In FY 2017, USCP changed its vulnerability management scanner from [redacted] to [redacted] In the beginning of FY 2018, the OIS refocused the patching and remediation process to resolve the top

ten patches that would remediate the most vulnerabilities as reported by [redacted] However, during FY 2018, OIS did not fully address remediation timeframes as described in USCP Directive [redacted], dated April 21, 2017. Additionally the USCP Standard Operating Procedure [redacted], dated April 27, 2017, states USCP should remediate legitimate vulnerabilities for Critical and High vulnerabilities in 5 and 15 days, respectively. Management was tracking the known vulnerabilities that had passed the remediation timeframe in a vulnerability dashboard.

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."

Recommendation 6: 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: Repeat Finding. Limited Progress.

Management Response: An update to the [redacted] is in progress which will include revisions to the response time by criticality requirements [redacted] OIS recently identified these timeframes as within our ability to meet and within industry expectations. Additionally, the implementation of continuous monitoring dashboards is providing security operation teams timely awareness.

It is expected that this revision will be provided to the Office of Policy and Management Systems within 30 days.

MLC 6: [redacted] (New Comment)

In FY 2017, USCP transitioned to the Architect of the Capitol instance of [redacted] As part of this change USCP had transitioned the [redacted] application administrative responsibilities in the prior year. However, during the current year the responsibilities of administrative actions including account review, review of security authorizations, and access management had not been fully defined or documented for the entire FY.

Additionally, account reviews had not occurred timely during the FY causing additional administrative accounts and access that were no longer required to exist for the majority of the FY.

During the current year review, several correction actions were noted including the identification of the system owner, data custodian and security points of contact.

The Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated September 2014, recommends management establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. Additionally it recommends as part of establishing an organizational structure, management considers how units interact in order to fulfill their overall responsibilities. Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities. Based on the nature of the assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, and related subunits. Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure.

Recommendation 7: We recommend that the United States Capitol Police implement a process to conduct [redacted] access and account reviews.

Recommendation 8: We recommend that the United States Capitol Police review the security authorization package for [redacted]

Status of Recommendation: New Finding.

Management Response: Concur. The development of an Organizational Level Agreement is complete and under OIS management review which will document the expectations, requirements, and responsibilities between OIS and System Owners. OIS expects to engage with the Office of Facilities and Logistics to have the agreement for [redacted] in place within 90 days and subsequently will be developing similar agreements with other system owners throughout FY 2019.

FY 2018 Status of Prior Year (FY 2017) Management Letter Comments

OIG reported seven comments in the FY 2017 Management Letter. We closed two of the MLCs, modified one and repeated four comments as shown below.

FY 2017 Comment No.	Comment	FY 2018 Status
1	[redacted] Database Change Control SOD Issues	Repeat Comment. See MLC 1.
2	Current Authorizations to Operate were not Documented	Repeat Comment. See MLC 2.
3	Monitoring of User Entity Controls	Closed
4	Purchase Card- Approving Official Did Not Sign Certification Report Forms	Modified Repeat Comment. See MLC 3.
5	Annual Performance Reports – Department Supervisors Did Not Complete or Return Annual Performance Reports to the OHR	Repeat Comment. See MLC 4.
6	Vulnerability Scanning and Review	Repeat Comment. See MLC 5.
7	Account Separation	Closed

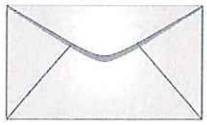
CONTACTING THE OFFICE OF INSPECTOR GENERAL

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