UNITED STATES CAPITOL POLICE

OFFICE OF INSPECTOR GENERAL

Management Letter
Related to the Audit of the United States Capitol Police's Fiscal Years 2019 and 2018 Financial Statements

Report Number OIG-2020-05

December 2019

~~*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

INSPECTOR GENERAL

December 13, 2019

MEMORANDUM

TO: Steven A. Sund
Chief of Police

FROM: Michael A. Bolton
Inspector General

SUBJECT: *Management Letter* (Report No. OIG-2020-05) *Related to the Audit of the United States Capitol Police's Fiscal Year 2019 Financial Statements* (Report No. OIG-2020-04)

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 Jacob Powell on [redacted]

Attachment: As stated.

cc: Assistant Chief Chad B. Thomas, Uniformed Operations
Assistant Chief Yogananda D. Pittman, Protective and Intelligence Operations
Mr. Richard Braddock, Chief Administrative Officer
[redacted] Audit Liaison

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

TABLE OF CONTENTS

Abbreviations and Acronyms

Construction in Progress	CIP
Credit Card Payments	CCP
Fiscal Year	FY
Library of Congress	LOC
Management Letter Comment	MLC
Material Weakness	MW
Notice of Findings and Recommendations	NFR
National Institute of Standards and Technology	NIST
Office of Acquisition Management	OAM
Office of Financial Management	OFM
Office of Human Resources	OHR
Office of Inspector General	OIG
Office of Information Systems	OIS
Performance and Evaluation Communication System	PECS
Purchase Card Holder/Approving Official Certification Report Form	Certification Report Form
Software as a Service	SaaS
Segregation of Duties	SOD
Standard Operating Procedure	SOP
Special Publication	SP
United States Capitol Police	USCP or the Department

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, 2019 and 2018, in accordance with auditing standards generally accepted in the United States of America, we considered USCP's internal control over financial reporting 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, 2019 in our *Independent Auditor's Report* dated December 13, 2019, (Report No. OIG-2020-04), 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 13, 2019.

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 9 findings related to the Fiscal Year (FY) 2019 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 13, 2019. We categorized 2 of 9 findings in the NFR matrix as MWs, and seven as MLCs. USCP's *Management Letter Related to the Audit of the United States Capitol Police's Fiscal Years 2018 and 2017 Financial Statements* (Report No. OIG-2018-05) identified six MLCs. We closed two of the previously reported MLCs, modified one and repeated three comments. OIG made three new findings during the FY 2019 financial statement audit.

Management Letter Comments

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

In Fiscal Year (FY) 2019, the Office of Information Systems (OIS) development team for [redacted] did not have proper SOD for its privileged users in the development and production environment. A single developer held the responsibility to develop and transfer code from development to production of the [redacted] environment.

The United States Capitol Police (USCP or the Department) has implemented capturing of the Windows Event Log for [redacted] database servers in the [redacted] This grants USCP the ability to review actions by user accounts. With a goal to act as a compensating control to monitor and remediate any SOD issues between development and production of [redacted] However, evidence supporting the review of user activities and code movement to production was not apparent.

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."

Due to the small [redacted] development group, inherent separation of duties issues exist. USCP has implemented limited tracking for privileged user activity on the [redacted] servers. However, [redacted] privileged database actions and functions exist without adequate monitoring to address compensating controls for SOD concerns. Without proper segregation of roles within the development environment of [redacted] unapproved changes may be made and released to the production environment of [redacted]

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. The full implementation of Segregation of Duties (SOD) requires the additional resources identified in the Test/Dev Environment Force Development Request. This request is approved and awaiting funding. In addition to the request, administrative actions are in progress to update the SOD matrix spanning across OIS disciplines and the creation of a Standard Operating Procedure specific to this finding identifying approved procedures mitigating the risk and possibility of an individual both creating custom code in a test environment and deploying that same code into production.

MLC 2: Multifactor Authentication was not Fully Implemented (New Comment)

The *Library of Congress* [redacted] *Cloud Memo on IT General Controls for Fiscal Year 2019*, identified USCP as having not implemented Multifactor Authentication for the [redacted] application.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*, control IA-2 enhancement 11 requires that, the information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the organization-defined strength of mechanism requirements.

Access to the [redacted] application has an increased risk of individual accounts being compromised by unauthorized individuals.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems and Office of Financial Management implement Multifactor Authentication methods to access the [redacted] application.

Status of Recommendation: New Comment

Management Response: Concur. The United States Capitol Police (USCP) is the customer of a cloud based software as a service (SaaS) implementation of [redacted] As such, any implementation of multi-factor authentication should be developed at the application layer for all SaaS customers. This approach has been discussed between the USCP and LOC Chief Information Officers and Chief Information Security Officers. The authentication process currently being proposed by Library of Congress (LOC) is not viewed by the Office of Information Systems (OIS) as true multi-factor authentication, rather a pass through authentication, which is redundant based on current architecture. Additionally, OIS is in the process of developing a multi-factor strategy for the Department, to include SaaS solutions, but has only implemented this requirement for on-premise privileged accounts to date.

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 to ensure compliance with USCP Standard Operating Procedure (SOP) [redacted], dated January 5, 2018.

A sample of 19 credit card payments (CCP) was tested as part of the FY 2019 financial statement audit. Multiple internal control exceptions were noted. For one transaction, the cardholder had not recertified their expired General Services Administration training prior to making a purchase. For seven transactions, the cardholder 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* and Citibank statement. For eight transactions, the purchase cardholder-approving official did not properly approve the Certification Report Form within the 9 day required period. For four transactions, the cardholders made a purchase prior to receiving approval on their purchase card request form.

The Department's process of monitoring cardholder's training was not operating effectively during FY 2019. Additionally, the Department's process of monitoring reconciliation packages for timeliness was not operating effectively during FY 2019. Finally, the Department's process for ensuring that purchase card requests are approved prior to making purchases was not operating effectively during FY 2019. Control weaknesses surrounding the process of monitoring the purchase card policies increases the risk of misstatement due to either fraud or error. Cardholders who do not recertify their training at the required intervals are at an increased risk of being unaware of current requirements for purchase cards. The untimeliness of the Certification Report Forms creates potential for errors in amounts paid by the Department. Additionally the lack of review by the approving official increases the risk for improper payments. Finally, making purchases prior to approval of purchase card requests increases the risk for improper purchases and puts the Department at risk for having purchases that exceed budgetary authority.

Recommendation 3: We recommend the United States Capitol Police continue to rigorously monitor purchase card policy controls.

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Concur. OAM will continue to review and ensure adequate USCP internal controls are in place and align with USCP policies that reflect best practices. OAM will continue to work with Card Holders and Approving Officials to ensure that Certification Forms are properly prepared and overall Purchase Card Program compliance is obtained and maintained.

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

The Department is not conducting employee performance evaluations and retaining evidence of the evaluations in employee personnel files as required by policies and procedures. Directive [redacted] dated October 15, 2018, contains the Department's guidance for the employee performance evaluation program. The directive requires annual performance expectation meetings between employees and supervisors, a mid-year performance review, a year-end self-assessment by the employee, and a year-end final summary rating.

The directive states that, "A copy of an employee's PECS Performance Planning and Appraisal Form (Final Summary Rating) will be retained in the employee's Central Personnel File."

The Office of Inspector General (OIG) selected a sample of 45 employees for internal control payroll testing. The Department's personnel folders did not contain performance evaluations in compliance with the directive for several of the 45 sampled employees. Examples of non-compliance that we noted included personnel files that did not contain performance evaluations completed within the last year, missing mid-year evaluations, evaluations that had not been signed by rating officials, and performance evaluations that did not include ratings. For example:

- 1 employee hired in 2009 had no performance evaluation in the personnel folder.
- 1 employee's most recent performance evaluation contained in the personnel folder was for 2008.
- 1 employee's most recent performance evaluation contained in the personnel folder was for 2010.
- 1 employee's most recent performance evaluation contained in the personnel folder was for 2012.
- 4 employees' most recent performance evaluation contained in the personnel folder was for 2013.
- 3 employees' most recent performance evaluation contained in the personnel folder was for 2014.
- 2 employees' most recent performance evaluation contained in the personnel folder was for 2015.
- 3 employees' most recent performance evaluation contained in the personnel folder was for 2016.

The Department is not enforcing its performance and evaluation policy requiring an evaluation to be performed for each employee annually. Additionally the Department is not maintaining evaluations in employee personnel files as required by the directive. Without conducting performance evaluations employees may not receive the feedback from management needed to perform their duties. Additionally, without properly preserved documentation of completed performance evaluations, the Department may lack support to effectively deal with performance related issues.

Recommendation 4: 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 them in personnel folders.

Status of Recommendation: Repeat Finding. No Progress.

Management Response: Generally concur. The PECS Directive, published on October 15, 2018, has mechanisms in place to monitor enforcement.

The Directive has a control in place that requires that 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. Further, 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 who have yet to receive a final summary rating, until compliance is reached.

While it is noted in the Directive that any delay in compliance with the requirements should be noted within the respective supervisors' performance appraisal for the appraisal period, the Department is considering different measures of performance evaluation criteria and escalating discipline to ensure full supervisory accountability for generating and closing out performance plans for their subordinates for each rating period.

MLC 5: Vulnerability Management Process Needs Improvement (Repeat Comment)

In FY 2018, OIS management had 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 2019 OIS Management did not fully address remediation timeframes as described in USCP Directive [redacted], dated April 21, 2017. Additionally, the USCP SOP [redacted] dated April 27, 2017, states that USCP shall remediate legitimate vulnerabilities for [redacted], 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 Organization*, control RA-5 states, "the organization: Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk."

OIS had changed the vulnerability scanning tool in the prior year which impacted the scan schedule and altered the remediation time frame as OIS continued to configure the scanning tool and work towards remediating vulnerabilities within required timelines. Additionally, OIS had identified, as a response to the prior year finding, that an update would be issued for SOP [redacted], which would revise the response times by criticality for timeframes identified by OIS that were within its abilities. However, this policy update had not been completed or put into place. USCP may have vulnerabilities with publically known compromises resulting in possible loss of department information.

Recommendation 5: 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: The Office of Information Systems (OIS) maintains an accurate account of open vulnerabilities and addresses them based on established criteria and implements mitigating controls as appropriate. Leveraging historical trending and risk

management practices, OIS will consult with the USCP Executive Team to determine the current criteria's applicability and achievability regarding the remediation of vulnerabilities with an emphasis on the critical and high vulnerabilities.

MLC 6: Unliquidated Obligations (New Comment)

The Department has an effective process of identifying obligations that need to be deobligated, however, the contract closeout and deobligation process is a lengthy, multi-step process. The Department does not have a process to recognize deobligations for financial reporting purposes for obligations that the Department knows need to be deobligated as of the end of the fiscal year, but for which the contract closeout/deobligation process has not been completed. Without such a process, unliquidated obligation balances listed on the Statement of Budgetary Resources may not be accurate.

During our testing, we identified $671,840 which should have been accrued for financial reporting purposes as of September 30, 2019. Additionally, at OIG's request, the Office of Financial Management (OFM) identified an additional $1,139,238 which should have been accrued for as of September 30, 2019. With these results, OFM posted an entry for $1,811,078 to ensure that the statements were reflected correctly.

The Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated September 2014, states that, "Management is directly responsible for all activities of an entity, including the design, implementation, and operating effectiveness of an entity's internal control system."

The Department lacks an internal control to ensure that unliquidated obligations awaiting the contract closeout/deobligation process are properly recognized for financial reporting purposes. Without such a control, the Department risks misstating their financial statements.

Recommendation 6: We recommend that the United States Capitol Police create a control to ensure that unliquidated obligations awaiting the contract closeout/deobligation process are properly recognized for financial reporting purposes.

Status of Recommendation: New Finding.

Management Response: Concur. OAM will continue to work with program offices to determine specific obligations that can be officially deobligated in the [redacted] financial system as of fiscal year-end. Additionally, OAM and program offices will develop a process to identify obligations which, although applicable close-out procedures are not yet complete, represent material amounts that are unlikely to result in future expenditures. Such amounts will be summarized and the summary amount reflected in the financial statements.

MLC 7: Construction in Progress (New Comment)

The Department does not have an effective process to ensure that Construction in Progress (CIP) is appropriately recognized in a timely manner. During our testing of a sample of 7 CIP additions, we noted one item for $499,852 which should have been recorded as an addition in FY 2018 instead of FY 2019. Specifically, the invoices related to the CIP addition were received and paid in FY 2018, but the accounting entry to recognize CIP was not made until FY 2019. OFM attempted to obtain the necessary information from the program office in order to record the CIP during FY 2018, however they did not receive a response until after the financial statements had been prepared.

We noted an additional item for $105,450 for which the related invoices are dated and were received during FY 2018, but the payment and recognition of CIP was made in FY 2019.

The Department does not have an effective process in place to ensure that responsible project offices overseeing CIP communicate to OFM the necessary information to record CIP in a timely manner. Additionally, the Department does not have effective procedures in place to educate project offices overseeing CIP projects on the importance of notifying OFM of the status of and updates to CIP projects prior to the end of the fiscal year. Without such processes, the Department risks materially misstating their financial statements.

Due to USCP not recognizing these purchases as CIP in a timely manner, the Property, Plant, and Equipment line on the Balance Sheet was understated as of September 30, 2018. Additionally, for the item which was paid in FY 2018 but recognized as CIP in FY 2019, Costs on the Statement of Net Cost were overstated as of September 30, 2018, and understated as of September 30, 2019.

Recommendation 7: We recommend that the United States Capitol Police implement a process to ensure that project offices communicate necessary information regarding recognizing Construction in Progress to the Office of Financial Management in a timely manner.

Recommendation 8: We recommend that United States Capitol Police implement procedures to educate project offices overseeing Construction in Progress projects on the importance of notifying OFM of the status of and updates to CIP projects in a timely manner.

Status of Recommendation: New Finding.

Management Response: Concur. USCP will review its procedures and communications around CIP additions to identify process improvements to support timely recognition of CIP additions. OFM will continue to review expenditure activity through the middle of the month following the reporting period for transactions applicable to CIP projects.

Communication efforts to program heads should describe the importance of timely reporting of costs incurred on CIP projects, especially during important cut off dates for financial reporting, (i.e. June 30 and September 30).

FY 2019 Status of Prior Year (FY 2018) Management Letter Comments

OIG reported six comments in the FY 2018 Management Letter. We closed two of the MLCs, modified one, and repeated three comments as shown below.

FY 2018 Comment No.	Comment	FY 2019 Status
1	[redacted] Database Change Control SOD Issues	Repeat Comment. See MLC 1.
2	Current Authorizations to Operate were not Documented	Closed
3	Purchase Cards – Certification Report Forms are not Properly Prepared	Modified Repeat Comment. See MLC 3.
4	Performance Reports – Not Completed and Returned to the Office of Human Resources	Repeat Comment. See MLC 4.
5	Vulnerability Scanning and Review (Titled "Vulnerability Management Process Needs Improvement" for FY 2019)	Repeat Comment. See MLC 5.
6	[redacted]	Closed

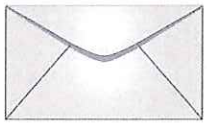
CONTACTING THE OFFICE OF INSPECTOR GENERAL

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 20003



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