Approved for Public Release by the Capitol Police Board on September 22, 2024

UNITED STATES CAPITOL POLICE

OFFICE OF INSPECTOR GENERAL

Management Letter
Related to the Audit of the United States Capitol Police's Fiscal Years 2021 and 2020 Financial Statements

Report Number OIG-2022-05

April 2022

~~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

April 22, 2022

OFFICE OF INSPECTOR GENERAL

MEMORANDUM

TO: J. Thomas Manger
Chief of Police

FROM: Michael A. Bolton
Inspector General

SUBJECT: *Management Letter* (Report No. OIG-2022-05) *Related to the Audit of the United States Capitol Police's Fiscal Years 2021 and 2020 Financial Statements* (Report No. OIG-2022-04)

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 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: Mr. Timothy Blodgett, Chief of Staff
Assistant Chief Yogananda D. Pittman, Protective and Intelligence Operations
Acting Assistant Chief Sean Gallagher, Uniformed Operations
Mr. Richard Braddock, Chief Administrative Officer
[redacted] Audit Liaison
[redacted] Executive Assistant

TABLE OF CONTENTS

Abbreviations and Acronyms

Approving Official	AO
Fiscal Year	FY
Information System Owner	ISO
Management Letter Comment	MLC
National Institute of Standards and Technology	NIST
Notice of Findings and Recommendations	NFR
Office of Acquisition Management	OAM
Office of Financial Management	OFM
Office of Information Systems	OIS
Office of Information Security – Radio Management Division	OIS-RMD
Office of Inspector General	OIG
Purchase Card Holder/Approving Official Certification Report Form	Certification Report Form
Separation of Duties	SOD
Standard Operating Procedure	SOP
United States Capitol Police	USCP or the Department
Vulnerability Management	VM

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, 2021, 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, 2021 and 2020 in our *Independent Auditor's Report* dated April 22, 2022, (Report No. OIG-2022-04), in which we communicated an unmodified opinion on internal control over financial reporting. However, during our audit the OIG became aware of control deficiencies that we do not consider to be material weaknesses or significant deficiencies, 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 April 22, 2022.

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 6 findings related to the Fiscal Year (FY) 2021 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, a significant deficiency, or a management letter comment (MLC). We categorized all six findings in the NFR matrix for FY 2021 as MLCs. USCP's *Management Letter Related to the Audit of the United States Capitol Police's Fiscal Years 2020 and 2019 Financial Statements* (Report No. OIG-2021-03) identified four MLCs. We closed one of the previously reported MLCs, and modified three comments. OIG made two new findings during the FY 2021 financial statement audit.

Management Letter Comments

MLC 1: Lack of Proper Accountability of Radio System (New Comment)

The Department does not have an effective process in place to properly account for and inventory the radio system.

The radio system, which the Department originally placed into service in 2014, carried a cost of $96M and a net book value of $48M at September 30, 2021. It comprised more than 71% of USCP's Property, Plant, and Equipment line of $67M on the September 30, 2021 financial statements. The Department accounted for the radio system as a single line item in the property management system, and did not include adequate detail for the major components of the system. The radio system asset was not included on any of the property custodians' annual inventory summary reports for FY 2021.

Additionally, the Property and Asset Management Division (PAMD) does not have a listing of the radio system components. PAMD referred the OIG to the Office of Information Security – Radio Management Division (OIS-RMD). While OIS-RMD does maintain lists of some of the components of the radio system, the Department does not have a comprehensive listing of the components of the radio system or a list of the major components of the radio system.

When the Department placed the radio system into service, per documentation in the accounting system supporting the transaction, the main components were [redacted] large outdoor antennas, over [redacted] indoor antennas, over [redacted] hand-held radios, and over [redacted] vehicle radios. OIS was able to provide us with some details for these components.

The Department maintains a listing of vehicle radios, however they do not keep it up-to-date. Upon inspection, OIG identified two vehicles that had radios installed, but were not included on the list. In one instance, the radio was not on the list at all, and in another instance, the radio was listed as being assigned to a different vehicle.

The Department is also not keeping their listing of hand-held radios up-to-date. For example, OIG noted three employees who had separated from the Department during FY 2021 who were still on the list as of November 10, 2021.

The Department was unable to provide a listing of the indoor antennas. Instead, the Department obtained maps of the Capitol complex buildings from the Architect of the Capitol with the indoor antennas annotated on them.

Although a substantial amount of the cost of the radio system was for non-physical items such as design, planning, labor, site buildout and preparation, installation, testing, etc., the Department does not track the larger, physical traceable components. However, when OIS-RMD provided the OIG with a tour of some of the major components of the radio system, we noted many items with USCP asset barcodes, indicating that barcoding and tracking of major components is feasible (and may have been intended during installation).

Recommendation 1: We recommend that the United States Capitol Police Property and Asset Management Division work with the Office of Information Systems to develop a list of critical components to the radio system and ensure that the critical components are inventoried on an annual basis.

Status of Recommendation: New Comment.

Management Response: Concur with the recommendation. The Office of Information Systems (OIS) will work with the Property and Asset Management Division (PAMD) to develop a list of critical components for annual inventory, as well as engage with the Office of Financial Management (OFM) on implications with respect to capitalization of the radio system.

MLC 2: Noncompliance with Employee Clock Usage Policy (Modified Repeat Comment)

OHR provided a report showing missing or no swipes (No Swipe Report) that reported 22,525 missing or no swipes related to 2,213 employees for our 12-month test period. This is down from the 58,180 missing or no swipes related to 1,979 employees for the 12-month test period during FY20. The No Swipe Report included the field "Comments" for personnel to enter explanations related to their timesheet. The No Swipe Report also included a field labeled "Reason" related to these missing swipes. Of the 22,525 missing swipes, 10,953 did not have a reason. This is down from 46,158 that did not have a reason in FY20. Of the 22,525 missing swipes with no reason, 6,957 also did not have a comment provided. This is down from 36,032 that did not have a comment provided in FY20.

From the sample of 45 employees, 27 employees had a total of 344 missing or no swipes. Reasons related to the missing swipes were: (1) forgot badge – 6, (2) forgot to swipe – 68, (3) misdirection – 35, (4) technical difficulty – 51, and most importantly, (5) no reason provided – 184. Of the 184 missing swipes with no reason, 115 also did not have a comment provided.

In addition to swiping procedures, employees are also required to attest to the time reported on their timesheets, and their supervisors are required to certify that time. These procedures provide additional control over the integrity of employee time and attendance. However, the remaining instances of unattested or uncertified time continue to pose a risk of inaccurate time and attendance records, particularly to the extent that unattested and uncertified time coincides with missing swipes.

Recommendation 2: We recommend the United States Capitol Police modify the time and attendance policy to include a sentence that explicitly refers to missing swipes:

"Supervisors are required to provide a reason that missed swipes occurred as well as comments for missing swipes, as necessary."

Recommendation 3: We recommend the United States Capitol Police (USCP) provide training to educate employees regarding Office of Human Resources policies and procedures including:

(a) the importance of clock swiping and identify it as part of their performance metrics in terms of being compliant with USCP policies; and

(b) how to properly use the clock swipes to reduce human errors when swiping, such as "misdirection" swipes, or incorrectly identifying a reason for offsite no swipes.

Recommendation 4: We recommend that United States Capitol Police (USCP) continue to monitor and enforce compliance with time and attendance policy over employee attestation and supervisor certification of timesheets.

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Concur with the recommendation. The USCP will update the Time and Attendance Directive to include the language, "Supervisors, or their designee, are required to provide a reason that missed swipes occurred as well as comments for missing swipes, as necessary". The Office of Human Resources (OHR) will collaborate with the Training Services Bureau (TSB) to deliver online training via APEX to educate employees on the policies and procedures related to swiping and how to properly utilize the clocks. The Department remains committed to the continued monitoring of and enforcement of required attestations and certifications.

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.

A sample of 14 credit card payments were tested as part of the FY 2021 financial statement audit. Multiple internal control exceptions were noted. For one sample, the cardholder did not properly reconcile the purchase card buying log to the Citibank statement. The approving official also signed off on the reconciliation package confirming proper completion. For two samples, the purchase card holder 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 three samples, the purchase cardholder-approving official did not properly approve the Certification Report Form within the 9 day required period.

<u>Recommendation 5</u>: We recommend the United States Capitol Police enforce the requirements of the Standard Operating Procedure [redacted]

Status of Recommendation: Modified Repeat Finding. Limited Progress.

Management Response: Concur with the recommendation. The Office of Acquisition Management (OAM) conducted [redacted] purchase card reconciliation training on March 18, 2022 for all cardholders with the [redacted] vendor, [redacted]. The training covered the reconciliation process for credit card statement lines and features of the Statement Reconciliation Notebook in [redacted]. The training extensively covered the overall reconciliation process to include reconciling the purchase card buying log to the Citibank Statement.

OAM will conduct reconciliation training for Approving Officials (AOs) and will emphasize AO responsibilities in accordance with SOP [redacted] and [redacted].

The current practice for late card holder submissions is for the card holder to notify the AO and AOPC in writing of the late submission prior to the due date and to include the notification in the purchase card package. OAM will update SOP [redacted] and [redacted] to include this practice.

<u>MLC 4</u>: Risk Management Framework Application Needs Improvement (New Comment)

USCP has a Risk Management policy as well as a Continuous Monitoring policy to provide guidance on the periodic assessment of information system controls against NIST 800-53 information system controls as part of the system security plan development and update. Controls that have not been implemented are documented in a POA&M; However, remediation or mitigation actions and timeframes are not developed for all POA&M items as some are left as "TBD."

As a result, certain weaknesses persist on the USCP network. For example,

- GSS and application accounts are not recertified on a routine (i.e. annual) basis.
- As noted in the FY19 audit (but not in the FY20 audit), [redacted] user accounts are not authenticated using multifactor authentication as encouraged by NIST 800-53 as well as required by the [redacted] Interagency Agreement with the Library of Congress.
- Although USCP has a formal change management directive, the directive refers to a specific, formal procedure that was still in a draft format as of the end of the FY. Several EGSS POA&M items relate to configuration and change management. None have a planned completion date.

Recommendation 6: We recommend that the United States Capitol Police Office of Information Systems require POA&M items to include specific timeframes and actions to be taken for POA&M item mitigation and remediation.

In addition, we recommend that USCP implement a process for maintaining, updating, and closing POA&M items within a specified amount of time.

Status of Recommendation: New Comment.

Management Response: Concur with the recommendation. OIS has published and distributed a [redacted]" document. A three tiered approach, in support of the [redacted], has been implemented and aligns to the process outline within NIST Risk Management Framework. The Compliance Team holds bi-weekly meetings with each USCP Information System Owner (ISO) and their support staff to review and discuss all open POA&M requirements. It is the responsibility of the information system security boundary's designated ISO to update POA&M milestones with executable remediation actions, achievable dates, and compensating controls as applicable.

OIS will ensure both the [redacted] handbook and the POA&M Management Process and Procedures documents identify milestone and timeline requirements and are disseminated to all USCP ISOs.

MLC 5: [redacted] Database Change Control Segregation of Duties Issue (Modified Repeat Comment)

In Fiscal Year (FY) 2020, the Office of Information Systems (OIS) development team for [redacted] did not have proper segregation of duties for its [redacted] in the [redacted] environment. A single developer held the responsibility to develop and transfer code from [redacted] of the [redacted] environment.

OIS established the [redacted] Standard Operating Procedures (SOP) on October 6th, 2020. While this SOP specifies the software development roles and responsibilities of the Enterprise Applications and Management Division Team while performing [redacted] application [redacted] deployments of code changes or system upgrades, USCP has not established a Separation of Duties matrix. Without an established Separation of Duties matrix USCP has not adequately identified incompatible duties and responsibilities performed by the Enterprise Applications and Management Division Team.

Recommendation 7: We recommend that the United States Capitol Police Office of Information Systems implement [redacted] development.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Concur with the recommendation. OIS will comply with NIST 800-53, Revision 4, AC-5 Separation of Duties (SOD), and take the necessary steps to update the [redacted] Standard Operating Procedures, and implement the following controls in support of [redacted] database change control:

a. Define and document duties of individuals to be separated by creating an SOD matrix; and

b. Define information system access authorizations to support separation of duties to include monitoring/auditing of separation.

MLC 6: Vulnerability Management Process Needs Improvement (Modified Repeat Comment)

In Fiscal Year (FY) 2020 OIS updated USCP Directive [redacted], dated July 23, 2020 and SOP [redacted] dated June 3, 2020 reflect achievable remediation timeframes including patching high risk vulnerabilities within [redacted], medium risk vulnerabilities within [redacted] and low risk vulnerabilities as determined by the CIO.

However, failure to remediate vulnerabilities in a timely manner still exists. [redacted]

[redacted] Additionally, as of the end of the FY, USCP Management was not following their Continuous Monitoring policy to accept the risk of persistent vulnerabilities that cannot be remediated within a timely manner.

Recommendation 8: We recommend that the United States Capitol Police Office of Information Systems address vulnerabilities in required timeframes or document mitigating controls and acceptance of risk.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Concur with the recommendation. OIS Information Security Division (ISD) provides bi-weekly reports of open vulnerabilities to all OIS support staff for remediation. In addition, there are bi-weekly meetings with the support personnel to discuss the vulnerabilities and assist with tracking the most critical assets needing remediation. It is the responsibility of the support staff to prioritize and remediate the discovered vulnerability within the timeframes listed within the Vulnerability Management (VM) SOP. OIS will continue to refine the VM process to ensure support staff are remediating vulnerabilities in accordance to the VM SOP.

FY 2021 Status of Prior Year (FY 2020) Management Letter Comments

OIG reported four comments in the FY 2020 Management Letter. We closed one of the MLCs, and modified three comments.

FY 2020 Comment No.	Comment	FY 2021 Status
1	Construction in Progress	Closed
2	Purchase Cards – Certification Report Forms are not Properly Prepared	Modified Repeat Comment. See MLC 2.
3	[redacted] Database Change Control Segregation of Duties Issue	Modified Repeat Comment. See IT MLC 2.
4	Vulnerability Management Process Needs Improvement	Modified Repeat Comment. See IT MLC 3.

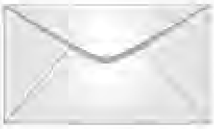
CONTACTING THE OFFICE OF INSPECTOR GENERAL

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.