UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Management Letter
Related to the Audit of the United States Capitol Police's Fiscal Years 2022 and 2021 Financial Statements

Report Number OIG-2023-03

December 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

December 9, 2022

OFFICE OF INSPECTOR GENERAL

MEMORANDUM

TO: J. Thomas Manger
Chief of Police

FROM: Ronald Gregory
Acting Inspector General

SUBJECT: *Management Letter* (Report No. OIG-2023-03) *Related to the Audit of the United States Capitol Police's Fiscal Year 2022 and 2021 Financial Statements* (Report No. OIG-2023-02)

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
Acting Assistant Chief Jason R. Bell, Protective and Intelligence Operations
Acting Assistant Chief Sean Gallagher, Uniformed Operations
Mr. Thomas A. DiBiase, General Counsel
Ms. Yogananda D. Pittman, Acting Chief Administrative Officer
[redacted] Audit Liaison
[redacted] Executive Assistant

TABLE OF CONTENTS

Abbreviations and Acronyms

[redacted]	[redacted]
Enterprise General Support System	EGSS
Fiscal Year	FY
[redacted]	[redacted]
Invoice Processing Platform	IPP
Management Letter Comment	MLC
National Finance Center	NFC
National Institute of Standards and Technology	NIST
Notice of Findings and Recommendations	NFR
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
Plan of Action and Milestones	POA&M
Property and Asset Management Division	PAMD
Purchase Card Holder/Approving Official Certification Report Form	Certification Report Form
Security Services Bureau	SSB
Standard Operating Procedure	SOP
System and Organization Controls	SOC
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, 2022, 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 opinion on the financial statements and reporting on internal control over financial reporting.

The Office of Inspector General (OIG) previously issued our opinion on USCP financial statements and report on internal control over financial reporting as of September 30, 2022 and 2021 in our *Independent Auditor's Report* dated December 9, 2022, (Report No. OIG-2023-02), in which we communicated that we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses or significant deficiencies. 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 December 9, 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 nine findings related to the Fiscal Year (FY) 2022 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 nine findings in the NFR matrix for FY 2022 as MLCs. USCP's *Management Letter Related to the Audit of the United States Capitol Police's Fiscal Years 2021 and 2020 Financial Statements* (Report No. OIG-2022-05) identified six MLCs. We closed none of the previously reported MLCs, and modified six comments. OIG made three new findings during the FY 2022 financial statement audit.

Management Letter Comments

MLC 1: Lack of Accountability of Property (Modified Repeat Comment)

The Department does not have an effective process in place to properly account for property. For property classified by the Department as a system, a single line item in the property management system accounts for all components and does not include adequate detail for the major components of the system. In FY 2021, OIG identified a radio system for which the Department did not have a listing of the radio system components. While the Office of Information Systems (OIS) did maintain lists of some of the components of the radio system, the Department did not have a comprehensive listing of all 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, but was unable to provide up-to-date listings of the vehicle radios and hand-held radios. In FY 2022, OIS provided a listing of major components for the radio system which included [redacted] comparators to account for the entire radio system.

Additionally, in FY 2022, OIG selected a sample of fifteen assets for testing and noted that two of the selected assets were also systems. These identified systems, the [redacted] system and [redacted] system, are tracked by the Department similarly to the radio system with one line item accounting for all components within the property system. The two systems are maintained by the Security Services Bureau (SSB), and all components related to these systems are tracked separately through the [redacted]

OIG reviewed the USCP Standard Operating Procedure (SOP) [redacted] dated April 30, 2012 and found the policy was last updated in 2012. Additionally, SSB confirmed that they do not reconcile [redacted], USCP's official system of record for all personal property, or properly perform inventories as required by the SOP. For example, SSB conducts a partial inventory annually; whereas, the SOP states a partial inventory will be conducted semi-annually and a wall-to-wall (complete) physical inventory annually.

Additionally, in performing procedures over the completeness of property records ("floor-to-book" testing), OIG selected a sample of fifteen active assets and found two of the assets had been disposed. One asset was disposed in 2011 and the other in 2022 however, the assets were still being tracked as active assets in the Department's records.

Finally, OIG selected a sample of five disposals and found that three of the five disposals did not have the proper verification and approval signatures on the disposal forms in accordance with Department policy.

The Department does not have a process in place to adequately identify and account for multi-component asset systems. Additionally, the Department does not have a process in place to maintain an adequate inventory of the items that comprise multiple item assets.

Although U SCPDirective [redacted], dated May 21, 2014 states items considered components of a capitalized system do not require a barcode, given the size, complexity, and cost of these critical systems, major components should be tracked and inventoried. Additionally, the policies and procedures for [redacted] are not maintained or utilized for proper tracking of assets related to SSB systems. Finally, the Department relies on the disposal specialist to report disposals to the Property and Asset Management Division (PAMD) as well as update the asset's current status in the property system. If the disposal specialist fails to inform PAMD or provide relevant forms to the Office of Financial Management after the disposal action is completed, the asset will remain in the Department's property balance as a current asset.

Without such processes to effectively track all property, the Departments risks materially misstating their financial statements as the Department replaces components or takes them out of service.

Recommendation 1: We recommend that the United States Capitol Police Property and Asset Management Division update Directive [redacted] dated March 29, 2022 to require additional accountability for components of systems and work with the responsible bureaus/offices to determine how critical components are identified, inventoried, and maintained related to these multi-item systems.

Recommendation 2: We recommend that the United States Capitol Police (USCP) Security Service Bureau update and enforce the USCP Standard Operating Procedure [redacted], dated April 30, 2012, to ensure that the [redacted] reconciliation and annual wall-to-wall inventory are performed.

Recommendation 3: We recommend that the United States Capitol Police Property and Asset Management Division enforce the USCP Directive [redacted], dated March, 29, 2022, to ensure that disposed assets are reported timely and all disposals are disposed of in accordance with Department policy.

Status of Recommendation: Modified Repeat Finding.

Management Response: Response 1: While Management understands the importance of the accountability of property, USCP does not concur with this recommendation as stated. As stated in U SCPDirective [redacted], a system asset is "two or more individual items (equipment components and parts) that are joined physically, electronically, or

electromechanically; are programmed or designed specifically to rely on each other; cannot function independently if separated; and cannot be easily disconnected and reconfigured to function with or within another until or "system." A system asset may have a central controller unit or hub and any number of remote or satellite stations/units and may serve more than one building or structure."

Although there are components specifically identified on the overall structure and design of a system, these are part of a "system" and are not recorded individually in the property management inventory system, [redacted], and will not separately received a barcode. Therefore the Department believes no additional steps are required by PAMD at this juncture.

Response 2: Management concurs with this recommendation. SSB will update Standard Operating Procedure [redacted] and will comply to the updated procedure regarding reconciliation of [redacted] and annual and semi-annual inventories (and will follow existing policy until updated).

Response 3: Management concurs with this recommendation. PAMD will enforce USCP Directive [redacted], especially as it pertains to disposals (Chapter 4 of Appendix A: Property and Asset Management Handbook). If any policy updates are needed regarding disposals, it will occur accordingly during our March review of the Directive..

MLC 2: Travel Undelivered Orders (New Comment)

The Department had an effective process of identifying most obligations that needed to be de-obligated, however, the Department did not separately consider and account for travel obligations at fiscal year-end. The Department did not have a process to de-obligate travel obligations or accrue them as delivered orders—when the travel has occurred—for financial reporting purposes. Without such a process, undelivered order balances reported on the Statement of Budgetary Resources may be overstated, Gross Costs on the Statement of Net Costs may be understated, and Accounts Payables on the Balance Sheet may be understated.

During our testing, we identified $7,747,000[1] in travel undelivered orders which should have been de-obligated or accrued as delivered orders for financial reporting purposes. Of that amount, $192,000 was de-obligated as part of a year-end undelivered order adjusting journal entry and $445,000 that was accrued as delivered orders in a year-end travel accounts payable accrual. The remaining $7,110,000 was included in the undelivered orders balance at September 30.

While management was reviewing the error to determine the necessary adjusting entries, they found that the Department had unpaid Citibank charges of $4,367,000. They factored this into the entry to correct the year-end travel undelivered orders and the travel accounts payable accrual.

[1] The figures presented in this management letter comment are rounded to the nearest thousand.

We assessed the impact of this error on the fiscal year 2021 financial statements and determined that no adjustment was necessary due to the materiality threshold.

The Department lacks an internal control to ensure that travel undelivered orders are properly evaluated and de-obligated or accrued as delivered orders for financial reporting purposes.

Without such a control, the Department risks misstating their financial statements.

> **Recommendation 4: We recommend that the United States Capitol Police develop and implement a control to ensure that open travel undelivered orders at year-end are properly evaluated and accounted for as either unobligated balances or delivered orders for financial reporting purposes.**

Status of Recommendation: New comment.

Management Response: Management concurs with the recommendation. USCP has updated its travel accrual estimate process, including travel de-obligations, for financial reporting purposes in Q4 FY 2022 and will continue to implement this update prospectively as well as update any related operating standard procedures to document this updated process.

MLC 3: Noncompliance with Employee Clock Usage Policy (Modified Repeat Comment)

The Office of Human Resources (OHR) provided a report showing missing or no swipes (No Swipe Report) that reported 30,858 missing or no swipes related to 1,028 employees for our 12-month test period. This is up from the 22,525 missing or no swipes related to 2,213 employees for the 12-month test period during FY 2021. 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 30,858 missing swipes, 19,197 did not have a reason. This is up from 10,953 that did not have a reason in FY 2021. Of the 30,858 missing swipes with no reason, 15,560 also did not have a comment provided. This is up from 6,957 that did not have a comment provided in FY 2021. The Department explained that missing swipes and swipes without reasons or comments are mainly isolated to a component of the Training Services Bureau.

From the sample of 45 employees, 36 employees had a total of 430 missing or no swipes. Reasons related to the missing swipes were: (1) forgot badge – 12, (2) forgot to swipe – 131, (3) misdirection – 59, (4) technical difficulty – 98, and most importantly, (5) no reason provided – 130. Of the 130 missing swipes with no reason, 98 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.

The Department does not enforce its employee clock usage policy. In addition, timekeepers are not utilizing the reason and comments fields when an employee misses a swipe. In many instances, the timekeeper enters a comment without completing the reason field. Further, the USCP Directive [redacted], dated April 4, 2019 does not include language requiring that employees or supervisors provide reasons and comments for missing swipes. "Missed Swipes" or "No Swipes" creates potential for payroll to be misstated. Employees may not have actually been present when they said they began work. The lack of enforcement creates a potential for fraud or misstatement of financial statements.

Recommendation 5: 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 6: 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 7: We recommend that United States Capitol Police continue to monitor and enforce compliance with time and attendance policy over employee attestation and supervisor certification of timesheets.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Response 1: Management concurs with the recommendation and will update USCP [redacted] as cited in the recommendation.

Response 2: Management concurs with the recommendation. Management continues to emphasize the importance and responsibilities of swiping and ensuring a missing swipe reason is indicated. The OHR will ensure this is continually included in the Timekeepers trainings.

Response 3: Management concurs with the recommendation. Compliance is monitored and Bureau Commanders/Office Directors receive regular reports of attestations and certifications needed and the importance of this process.

MLC 4: Payroll Documentation (New Comment)

The Department does not always retain employee personnel documentation in Central Personnel Files as required by policies and procedures. Additionally, the Standard Operating Procedure related to Central Personnel Files was last updated May 28, 2012.

As part of the new-hire and separated employee internal control testing procedures, OIG selected a sample of 39 new hires. The Department's personnel folders did not contain completed Form I-9s, *Employment Eligibility Verification*, for 4 of the samples.

Additionally, OIG selected a sample of 45 employees for internal control and payroll detail testing. The Department's personnel folders did not contain a Federal Employee Group Life Insurance form for 1 of the sampled employees. The employee had selected Basic and Standard coverage, and the Department is required to maintain signed forms for employees who select anything more than Basic coverage. OIG informed OHR of the missing form and OHR is working on obtaining a new completed form from the employee.

Of the sample of 45 employees, OIG also noted that the Department's personnel folders did not contain performance evaluations in compliance with the related directive for 5 employees. Examples of non-compliance that we noted included:

- 1 employee hired in 2018 had no performance evaluations.
- 2 employee's most recent performance evaluation on file was from 2018.
- 2 employee's most recent performance evaluation on file was from 2019.

The Department is not retaining employee personnel documentation in Central Personnel Files as required by policies and procedures. The Department is not enforcing its [redacted] directive requiring a copy of employees' final annual evaluations to be retained in their Central Personnel File. As of November 8, 2022, the Department updated this directive and going forward evaluations will be maintained in APEX[2]. The Department has an outdated policy for Central Personnel File maintenance that does not include a list of required documents.

Incomplete Central Personnel Files subject the Department to uncertainty if there is a personnel issue. It exposes the Department to a heightened possibility of long-term litigation risks for failure to maintain personnel records. Not maintaining I-9 Forms is a violation of the United States Citizenship and Immigration Services requirement to complete and maintain the forms.

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.

[2] APEX is a learning and talent management web application that supports USCP Learning/Training, Performance, and Recruiting functions.

Recommendation 8: We recommend the United States Capitol Police update Standard Operating Procedure [redacted] dated May 28, 2012. The update should include a list of documents the Office of Human Resources is required to maintain in the Central Personnel Files.

Recommendation 9: We recommend the United States Capitol Police ensure compliance with the new performance evaluation directive, which requires records to be available to employees, supervisors, and the Office of Human Resources in APEX.

Status of Recommendation: New Comment.

Management Response: Response 1: Management concurs with this recommendation and will update Standard Operating Procedure [redacted] with the list of documents required to be maintained in the Central Personnel Files.

Response 2: Management concurs with this recommendation and will ensure compliance with Directive [redacted]

MLC 5: Purchase Cards – Certification Report Forms 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 18 credit card payments were tested as part of the FY 2022 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 five 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 (Purchase Log) and Citibank statement. For three samples, the purchase cardholder-approving official did not properly approve the Certification Report Form within the 10 day required period.

The Department's process of monitoring reconciliation packages for timeliness was not operating effectively during FY 2022. Additionally, the Department's process for ensuring that purchase card requests are approved prior to making purchases was not operating effectively during FY 2022. Control weaknesses surrounding the process to monitor the purchase card policies increases the risk of misstatement due to either fraud or error. 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.

Recommendation 10: We recommend the United States Capitol Police enforce the requirements of the Standard Operating Procedure [redacted], dated September 21, 2020.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Management concurs with this recommendation and will continue to strive for full compliance with Standard Operating Procedure [redacted].

MLC 6: Risk Management Framework Application Needs Improvement (Modified Repeat 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 Plan of Action and Milestones (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,

- [redacted].
- [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 Enterprise General Support System (EGSS) POA&M items relate to configuration and change management. None have a planned completion date.

In addition, during the FY 2022 audit, we determined that USCP was not including all identified exceptions from the EGSS system security plan in the EGSS POA&M. Specifically, control [redacted] was not implemented. This occurred because USCP is updating the POA&M based off of the annual security assessment report. Control [redacted] was not included in the most recent security assessment plan or security assessment report.

Furthermore, USCP has not defined a continuous monitoring strategy that includes a determination or method of selecting controls to be monitored and periodically assessed. Neither the [redacted] or [redacted] provide prescriptive guidance on how to apply the RMF as it relates to continuously monitoring security controls in place.

Recommendation 11: We recommend that the United States Capitol Police Office of Information Systems provide guidance for selecting controls to be assessed as part of the continuous monitoring program.

Recommendation 12: We recommend that the United States Capitol Police Office of Information Systems require Plan of Action and Milestones (POA&M) items to include specific timeframes and actions to be taken for POA&M item mitigation and remediation.

Recommendation 13: We recommend that the United States Capitol Police implement a process for maintaining, updating, and closing Plan of Action and Milestones items within a specified amount of time.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Response 1: Management concurs with this recommendation. USCP has documented a Plan of Action and Milestone management process to support the continuous monitoring of POA&Ms within the information system security boundary and a [redacted] handbook to support the core control assessments. And will continue to update the Continuous Monitoring policy as needed for assessing controls.

Responses 2 and 3: Management concurs with this recommendation and the "Plan of Action and Milestone Management Processes and Procedures" document will be reviewed and updated.

MLC 7: [redacted] Database Change Control Segregation of Duties Issue (Modified Repeat Comment)

OIS development team for [redacted] did not have proper segregation of duties for its [redacted] in the [redacted] environment. A [redacted] held the responsibility to develop and transfer code from [redacted] of the [redacted] environment.

OIS established the [redacted] 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 a Separation of Duties matrix USCP has not adequately identified incompatible duties and responsibilities performed by the Enterprise Applications and Management Division Team.

Recommendation 14: We recommend that the United States Capitol Police Office of Information Systems implement [redacted] development.

Status of Recommendation: Repeat Finding. Limited Progress.

Management Response: Management concurs with the recommendation and will update the [redacted] Standard Operating Procedure to ensure that we continue mitigating this finding

MLC 8: Vulnerability Management Process Needs Improvement (Modified Repeat Comment)

In 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 Chief Information Officer.

However, failure to remediate vulnerabilities in a timely manner still exists. [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 15: 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: Management concurs with the recommendation. OIS will continue to refine the VM [Vulnerability Management] process to ensure support staff are remediating vulnerabilities in accordance to the VM SOP, including [redacted] of vulnerabilities.

MLC 9: Third Party Service Provider Oversight Needs Improvement (New Comment)

USCP does not review sub-service organization System and Organization Controls (SOC) reports. Specifically,

[redacted]

[redacted]

In addition, USCP does not meet all of the requirements of the third-party service provider agreements. Specifically, USCP has not implemented two-factor authentication as required by their [redacted] service agreement with the Library of Congress.

Recommendation 16: We recommend that the United States Capitol Police (USCP), Property Asset Management Division, Office of Human Resources, and Office of Financial Management, in coordination with the Office of Information Systems, request the [redacted]

- **USCP should review the SOC reports and consider how any exceptions noted in the report may impact USCP and any mitigating controls that might need to be implements.**
- **USCP should also review the SOC reports and monitor all complementary entity user controls that USCP is responsible for managing.**

Recommendation 17: We recommend that the United States Capitol Police (USCP) review all third-party service provider agreements to ensure compliance with USCP responsibilities.

Status of Recommendation: New Comment.

Management Response: Response 1: USCP concurs with this recommendation and will seek SOC reports as cited and assess and address, if needed, any vulnerabilities cited.

Response 2: USCP concurs with this recommendation. USCP will continue improving the review of third-party service provider agreements.

FY 2022 Status of Prior Year (FY 2021) Management Letter Comments

OIG reported six comments in the FY 2021 Management Letter. We closed none of the MLCs, and modified six comments.

FY 2021 Comment No.	Comment	FY 2022 Status
1	Lack of Proper Accountability of Radio System	Modified Repeat Comment. See MLC 1.
2	Noncompliance with Employee Clock Usage Policy	Repeat Comment. Limited Progress. See MLC 3.
3	Purchase Cards – Certification Report Forms are not Properly Prepared	Repeat Comment. Limited Progress. See MLC 5.
4	Risk Management Framework Application Needs Improvement	Repeat Comment. Limited Progress. See MLC 6.
5	[redacted] Database Change Control Segregation of Duties Issue	Repeat Comment. Limited Progress. See MLC 7.
6	Vulnerability Management Process Needs Improvement)	Repeat Comment. Limited Progress. See MLC 8.

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