UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Follow-up on
United States Capitol Police
Controls over Proximity Cards

Report Number OIG-2018-13

June 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 Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

OFFICE OF INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports OIG prepares periodically as part of its oversight responsibility with respect to the United States Capitol Police (USCP) to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office or function under review. Our work was based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG and discussed the draft findings with those responsible for implementation. It is my hope that the recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to those contributing to the preparation of this report.

Michael A. Bolton
Acting Inspector General

TABLE OF CONTENTS

Abbreviations and Acronyms

Clearance Definition Report	CDR
Fiscal Year	FY
Government Accountability Office	GAO
Office of Background Investigation and Credentialing	OBIC
Office of Human Resources	OHR
Office of Inspector General	OIG
Proximity	Prox
Security Services Bureau	SSB
Standard Operating Procedures	SOP
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

In a previous audit, *Performance Audit of USCP Controls over Proximity Cards,* Report Number OIG-2015-05, dated April 2015, the Office of Inspector General (OIG) found the United States Capitol Police (USCP or the Department) did not have effective controls over the process for proximity (prox) cards. To develop more effective controls over the process, OIG made five recommendations, which the Department agreed to implement. As of September 17, 2015, the Department had fully implemented four recommendations based on comments and documentation provided to OIG. At the start of this engagement, one recommendation remained open.

In February 2017, the Government Accountability Office (GAO) updated its *High Risk Series,* GAO-17-317, which states that the Federal Government could do more to improve the capacity and monitoring of physical security. In response to GAO, OIG conducted a follow-up on the Department's implementation of recommendations contained within Report Number OIG-2015-05. The objectives of this follow-up were to confirm that the Department took the appropriate corrective actions and that controls the Department implemented were operating efficiently and effectively. Our scope included existing controls over prox cards for Fiscal Year (FY) 2017 through February 28, 2018, related to implementation of recommendations outlined in our previous report.

We conducted interviews and reviewed relevant documentation to gain an understanding of the Department's implementation of recommendations. When we began this engagement, Recommendation 1 of the previous report remained open. During the engagement, we identified lapses in corrective actions that impaired the closed status of the other four recommendations. Based on our work, the conditions identified in the previous audit re-emerged as a result of a lack of continuity in the Department's corrective actions. Prior to issuance of the final report, the Department updated a directive and issued a new standard operating procedure (SOP) that affected Recommendation 1 in the prior report. OIG reviewed the updated directive and new SOP and concluded that the Department designed the procedures appropriately to mitigate the deficiency noted in the prior report and this follow-up report. Thus, OIG closed Recommendation 1 from the earlier report.

During the follow-up, however, we identified other matters that warranted the Department's attention. For example, we reviewed a sample of separation checklists and noted that of the 12 samples reviewed, 2 used outdated checklists that did not include a sign-off signature line for the Security Services Bureau (SSB). We also noted instances in which data within the prox card systems were not accurate.

On May 25, 2018, we provided a draft report to the Department for comment and attached their response in its entirety in Appendix B.

BACKGROUND

In previous work, *Performance Audit of USCP Controls Over Proximity Cards,* Report Number OIG-2015-05, dated April 2015, the Office of Inspector General (OIG) found that the United States Capitol Police (USCP or the Department) did not have effective controls over the process of proximity (prox) cards. The Department's internal controls over separated and transferred employees were not effective and resulted in separated and transferred employees maintaining inappropriate access with prox cards. Additionally, the Department had inadequate policies and procedures surrounding the process for prox cards. OIG identified inadequate controls over access clearances.

To establish more efficient and effective controls over the process for prox cards, we made five recommendations, which the Department agreed to implement. As of September 17, 2015, OIG had closed four of the five recommendations from the 2015 audit based on comments and documentation provided by the Department.

The Security Services Bureau (SSB) is responsible for the majority of the processing for prox cards. When new employees and contractors start work with USCP, security managers from other Department bureaus request prox card access from SSB. SSB grants the prox card access. When separating from the Department, employees and contractors must complete a separation checklist, which includes a section SSB completes. The separation checklist is SSB's primary means for determining if an employee has separated. The Office of Human Resources (OHR) actually issues the prox cards, which also serve as building access cards, when needed and collecting cards when employees terminate.

SSB uses [redacted] software to administer prox cards. [redacted] is a commercial grade, scalable security management solution capable of monitoring multiple card readers and accounting for many cardholders at a given time. During the scope of our follow-up, SSB was upgrading from [redacted] to [redacted]. During the upgrade, SSB identified technical difficulties because of coding issues. As a result of those difficulties, SSB did not fully implement the upgrade and is waiting for the developer to fix the coding. Until the developer finishes updating the code, SSB will use both [redacted] and [redacted].

OBJECTIVE, SCOPE, AND METHODOLOGY

In February 2017, the Government Accountability Office (GAO) updated its *High Risk Series,* GAO-17-317, which states that the Federal Government could do more to improve capacity and monitoring of physical security. In response to GAO, OIG conducted a follow-up review on the Department's implementation of recommendations contained within Report Number OIG-2015-05. Our objectives of the follow-up were to confirm that the Department took the appropriate corrective actions and that controls the Department implemented were operating efficiently and

effectively. Our scope included existing controls over prox cards for Fiscal Year (FY) 2017 through February 28, 2018, related to implementation of recommendations outlined in our previous report.

To accomplish our objectives, we interviewed Department officials. We also reviewed documentation provided by the Department in order to determine the status of the prior recommendations. We reviewed Report Number OIG-2015-05 as well as correspondence between OIG and USCP related to closure of the recommendations included in the report. Additionally, we reviewed:

- Relevant policies and procedures related to prox cards
- SSB Clearance Definition Reports (CDRs[1])
- Lists of employees OHR provided
- Separation checklists of employees leaving the Department

OIG conducted this analysis in Washington, D.C., from February through May 2018. We did not conduct an audit, the objectives of which would be the expression of an opinion on Department programs. Accordingly, we do not express such an opinion. Had we performed additional procedures, other issues might have come to our attention that we would have reported. ~~This report is intended solely for the information and use of the Department, the USCP Board, and USCP Oversight Committees and should not be used by anyone other than the specified parties.~~

RESULTS

Our follow-up identified lapses in corrective actions that impaired the closed status of several recommendations. Additionally, OIG identified other matters related to prox cards that warranted the Department's attention.

Status of Previous Recommendations

In a previous audit (Report Number OIG-2015-05), OIG found the Department did not have effective controls over the process for prox cards. To develop more efficient and effective controls over that process, OIG made five recommendations, which the Department agreed to implement. Prior to the start of our work, the Department provided OIG with corrective actions for four of the five recommendations, and OIG subsequently closed four. When we began this follow-up in February 2018, Recommendation 1 was the only recommendation still open. OIG

[1] A CDR is a report generated by SSB, which is sent to bureau security managers. Security managers utilize the report to ensure that individuals with access to the doors for which they are responsible have appropriate access.

subsequently identified lapses in corrective actions that impaired the status of the four closed recommendations. Based on our follow-up, the conditions identified in the previous audit re-emerged because a lack of continuity existed in the Department's corrective actions. Prior to OIG issuing this report, the Department updated a directive and a standard operating procedure (SOP) affecting Recommendation 1. OIG reviewed the updated directive and new SOP and concluded that the Department designed the procedures to mitigate the deficiency noted in the previous audit and this review. OIG closed Recommendation 1. See the prior recommendations along with their status below:

Previous Recommendation 1: We recommend that the United States Capitol Police update the Office of Human Resources (OHR) policies and procedures related to proximity cards and require the Security Services Bureau (SSB) to remove access clearances for separated employees when notified by the OHR badging office. Policies should specifically state a required timeframe for OHR communication and SSB access removal.

When this review began, the Department had not finalized the SOP.

USCP did not maintain adequate controls over prox cards for employees who separated from the Department. Of the 162 employees who separated from the Department during FY 2017 through February 28, 2018, we determined that 35 prox cards remained active. Of the 35 prox cards, 20 maintained access to bureau-specific doors,—access that bureaus were required to review on quarterly CDRs. Of the 35 prox cards, 33 maintained access to default access doors to which all USCP employees had access, such as the east door of the USCP Headquarters Building. According to an official in the Office of Background Investigation and Credentialing (OBIC), 34 of the 35 prox cards were returned to OBIC. The 35th card had been reported as lost/stolen.

Prior to the issuance of this report, the Department updated Directive [redacted] dated May 14, 2018, requiring that OBIC notify SSB immediately when a separating employee returns their prox card and issued SOP [redacted] dated May 14, 2018, which requires that OBIC notify SSB when any card is lost or stolen. OIG reviewed the updated directive and new SOP, and concluded that the Department designed the procedures in such a way that would mitigate the deficiency noted during our follow-up. OIG, therefore, closed Recommendation 1 from the previous report.

Previous Recommendation 2: We recommend that the United States Capitol Police update the Security Services Bureau (SSB) policies and procednres to direct security managers to provide SSB with confirmation that offices and Bureaus have reviewed the quarterly reports for accuracy.

The Department updated Directive [redacted] dated September 30, 2015, to include instructions for security managers to review and validate any access list associated with access clearances on a quarterly basis, and notify the SSB upon

completion. Additionally, the Directive included instructions on how to assist security managers in reviewing and validating the access lists.

The Department, through SSB, generates CDRs, which SSB must provide each quarter to security managers of the bureaus within the Department.

Security managers were not consistently returning completed responses to SSB. Although it provided OIG with 73 quarterly reports sent to security managers during the scope of this follow-up, SSB was able to provide only 3 responses from security mangers. The three responses included a request for access removal based on review, a clarification on the received report requesting a "complete report," and a response simply stating "Thank you." See new recommendation below.

Previous Recommendation 3: We recommend that the United States Capitol Police finalize draft Security Services Bureau Standard Operating Procedures to include providing training to individuals when initially designated as a security manager, then on a yearly basis thereafter.

The Department updated Directive [redacted] instructing SSB to reflect the requirement for providing newly appointed security managers initial training as well as annual training.

SSB provides new security managers with a training tutorial document; however, SSB did not provide annual refresher training as Directive [redacted] requires. According to a Department official, SSB plans to formalize training by the end of FY 2018. See new recommendation below.

Previous Recommendation 4: We recommend that the United States Capitol Police, Security Services Bureau (SSB) send quarterly *Clearance Access Definition Reports* to security managers consistently and timely for their review. SSB should track the status of the review and confirmation process and maintain evidence of the process.

According to a Department official, SSB maintains a Microsoft Excel spreadsheet for logging each response received from security managers. SSB generates and submits quarterly CDR reports and receives some responses from security managers.

However, because of difficulties regarding software upgrades within SSB, CDR reports were not consistently generated for security managers during the scope of this follow-up. According to SSB officials, the bureau was working with the software developer, and expects new code to resolve upgrade issues by June 2018. See new recommendation below.

Previous Recommendation 5: We recommend that the United States Capitol Police security managers provide information related to the individual's employing office to the Security Services Bureau (SSB). Further, SSB should confirm that requests from security managers are complete (all data fields populated) before granting access privileges.

The Department updated [redacted] to include guidance requiring that SSB will provide access only when the Security Access Controls forms are completed. The Directive also requires that employees complete forms fully and accurately prior to any action from SSB.

OIG selected a sample of 10 new employees to ensure that employees and security managers properly completed forms before SSB granted prox card access. SSB could not provide the forms for 9 of the 10 sampled employees. According to an SSB official, they are formalizing and documenting a new process to require that all completed request forms are properly categorized and more searchable. See new recommendation below.

Conclusion

Based on our follow-up, the conditions identified in the previous audit re-emerged because a lack of continuity existed in the Department's corrective actions. Thus, OIG issues four new recommendations.

Recommendation 1: We recommend that the United States Capitol Police identify additional measures to ensure compliance with Directive [redacted] dated September 30, 2015, which requires that security managers respond to the Security Services Bureau when receiving Clearance Definition Reports.

Recommendation 2: We recommend that the United States Capitol Police identify additional measures for ensuring compliance with Directive [redacted] which requires that the Security Services Bureau provide annual training to security managers.

Recommendation 3: We recommend that the United States Capitol Police, Security Services Bureau send quarterly Clearance Definition Reports to security managers consistently and timely for review. The Security Services Bureau should track the status of the review and confirmation process and maintain evidence of the process. Additionally, if the Security Services Bureau does not receive a response it should follow-up with the security manager and escalate the request with the security manager's chain of command until they receive a response.

Recommendation 4: We recommend that the United States Capitol Police ensure compliance with Directive [redacted], which requires that employees and security managers complete access control forms before the Security Services Bureau grants proximity card access. Additionally, the Security Services Bureau should develop a system to maintain completed forms.

Other Matters

During the follow-up, OIG also identified other matters that warranted the Department's attention. For example, of the 12 separation checklists reviewed, 2 contained either outdated or obsolete, or both, separation checklists that did not include a sign-off line for SSB. OIG noted instances in which data within the prox card system were not accurate.

Inconsistent Separation Checklist/Process

OIG conducted testing to confirm separated employees returned prox cards, and the Department appropriately removed prox card access through the separated employee process. Of the 12 checklists sampled, 2 separated employees used either outdated or obsolete [redacted], which did not include the required new sections where SSB could sign off. SSB did not terminate prox card access for one employee upon separation.

Data Accuracy

The information entered in the prox card system for two individuals was not accurate. For one individual, the last name was not correct and the second employee—a civilian—was listed as a contractor on one CDR and as a sworn officer on another.

Such data accuracy issues came to our attention while following up on the prior recommendations. We did not perform specific testing over data accuracy. If we had performed data accuracy testing, other instances may have come to our attention.

Conclusion

The Department did not ensure data accuracy in the [redacted] system and failed to consistently use an up-to-date [redacted]. Failure to maintain data accuracy and follow a consistent and repeatable separation process increases the risk of security breaches within the Capitol campus.

Recommendation 5: We recommend that the United States Capitol Police ensure that employees use the most up-to-date [redacted].

Recommendation 6: We recommend that the United States Capitol Police create policies or procedures that will ensure the accuracy of proximity card data.

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police identify additional measures to ensure compliance with Directive [redacted] dated September 30, 2015, which requires that security managers respond to the Security Services Bureau when receiving Clearance Definition Reports.

Recommendation 2: We recommend that the United States Capitol Police identify additional measures for ensuring compliance with Directive [redacted] which requires that the Security Services Bureau provide annual training to security managers.

Recommendation 3: We recommend that the United States Capitol Police, Security Services Bureau send quarterly Clearance Definition Reports to security managers consistently and timely for review. The Security Services Bureau should track the status of the review and confirmation process and maintain evidence of the process. Additionally, if the Security Services Bureau does not receive a response it should follow-up with the security manager and escalate the request with the security manager's chain of command until they receive a response.

Recommendation 4: We recommend that the United States Capitol Police ensure compliance with Directive [redacted] which requires that employees and security managers complete access control forms before the Security Services Bureau grants proximity card access. Additionally, the Security Services Bureau should develop a system to maintain completed forms.

Recommendation 5: We recommend that the United States Capitol Police ensure that employees use the most up-to-date [redacted].

Recommendation 6: We recommend that the United States Capitol Police create policies or procedures that will ensure the accuracy of proximity card data.

DEPARTMENT COMMENTS

UNITED STATES CAPITOL POLICE

OFFICE OF THE CHIEF

119 D STREET, NE

WASHINGTON, DC 20510-7218

June 11, 2018

COP 180239

MEMORANDUM

TO: Mr. Michael A. Bolton
Acting Inspector General

FROM: Matthew R. Verderosa
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Follow-up on United States Capitol Police Controls over Proximity Cards* (Report No. OIG-2018-13)

The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of Inspector General's (OIG) draft report *Follow-up on United States Capitol Police Controls over Proximity Cards* (Report No. OIG-2018-13).

The Department generally agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon current policies and procedures currently in place within the Department's proximity card process. The Department will assign Action Plans to appropriate personnel regarding each recommendation in effect to achieve long term resolution of these matters.

Thank you for the opportunity to respond to the OIG's draft report. Your continued support of the women and men of the United States Capitol Police is appreciated.

Very respectfully,

Matthew R. Verderosa
Chief of Police

cc: Steven A. Sund, Assistant Chief of Police
Richard L. Braddock, Chief Administrative Officer
[redacted] USCP Audit Liaison

Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.

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 – we are located at:
United States Capitol Police
Attn: Office of Inspector General, Investigations
119 D Street, NE
Washington, DC 20510

Or visit us – we are located at:
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