Approved for public release by the Capitol Police Board on September 3, 2025

UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Performance Audit of USCP Controls Over Proximity Cards

Report Number OIG-2015-05

April 2015

Notice – Distribution of This Document Is Restricted

This report is intended solely for the official use of the United States Capitol Police, or 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 prior authorization by the Inspector General or the Capitol Police Board.

UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003

INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) contracted with Cotton & Company LLP (Cotton) to conduct a performance audit and prepare 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. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and review of applicable documents.

Cotton, in coordination with OIG, developed recommendations based on the best knowledge available at the time and discussed 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.

Fay F. Ropella

Fay F. Ropella, CPA, CFE
Inspector General

This page intentionally left blank

TABLE OF CONTENTS

Abbreviations

Access Clearance Definition Reports	quarterly reports
Cotton & Company LLP	Cotton
Fiscal Year	FY
National Institute of Standards and Technology	NIST
Office of Human Resources	OHR
Office of Inspector General	OIG
Proximity Cards	prox cards
Radio Frequency Identification	RFID
Security Services Bureau	SSB
Special Publication	SP
Standard Operating Procedure	SOP
Structured Query Language	SQL
United States Capitol Police	USCP
United States House of Representatives	House

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) uses proximity (prox) cards to control access to security objects. Security objects include items such as doors, card readers, people, and related items associated with secured areas. Prox cards mitigate the risk of destruction or misappropriation of agency assets or data within secured areas.

The USCP Office of Inspector General (OIG) contracted with the independent public accounting firm Cotton & Company LLP (Cotton) to conduct a performance audit of USCP prox cards. The objectives of the performance audit were to determine (1) the effectiveness of USCP's internal control over prox cards to ensure accountability of those sensitive items, and (2) whether USCP complied with applicable policies and procedures as well as applicable laws and regulations. Cotton was to follow up, if applicable, on the status of previous recommendations the OIG for the U.S. House of Representatives (House OIG) made. Our scope included controls, processes, and operations related to USCP controlled security objects for fiscal year (FY) 2014.

Prox cards are an important resource and when used properly, can significantly reduce security risks. However, the controls over the prox card process have not been effective. In response to the House OIG audit recommendations, the Security Services Bureau (SSB) drafted the [redacted] Standard Operating Procedure (SOP) in 2011 to outline the role of a security manager and to define controls related to prox cards. USCP has used the SOP as a best practice since its inception. The Department has not; however, formally adopted the SOP. And although the Department has used the SOP as guidance since 2011, the document needs improvement.

The [redacted] SOP outlines the role of security managers and the role of SSB as the access administrator. Neither role is charged with providing positive assurance that the controls are functioning properly. In particular, security managers are responsible for controlling security objects, people, and access lists in a particular security area. Responsibility includes approving, revoking, and maintaining access clearances within their purview.

This audit revealed that multiple instances existed of employees who continued to have access despite separation or transfer. According to the SOP, SSB is responsible for removing access when a security manager notifies SSB, and [redacted] dated August 20, 2009, requires that the Office of Human Resources (OHR) badging office send electronic notification to SSB when an employee returns their prox card. The SOP, however, does not specifically address employees who have separated from the Government or transferred from one job to another.

The SOP states that SSB must provide quarterly *Clearance Access Definition Reports* (quarterly reports) to security managers for review and that the security managers "shall review and validate all access lists associated with their access clearances on a quarterly basis, at a minimum." For the four quarters tested during FY 2014, SSB could not provide documentation that it consistently provided those reports to security managers. The SOP also does not require that the security manager confirm completion of the review of the quarterly reports. The SOP states that the security manager should inform SSB of any changes to access clearances. Testing revealed that security managers were not thoroughly reviewing the quarterly reports.

We were unable to evaluate compliance because the Department has yet to finalize the revised policies and procedures.

Background

The United States Capitol Police (USCP or the Department) is a law enforcement agency within the legislative branch of the Federal Government, which is tasked with protecting the Capitol Complex and Members of Congress domestically and abroad. To control access to secure locations across the Capitol Complex, USCP uses proximity cards (prox cards). These cards are plastic cards enabling keyless access.

The U.S. House of Representatives (House) Office of Inspector General (OIG) conducted a physical security review of the [redacted] located in Washington, D.C. The review concluded that a security weakness existed with respect to the security managers, who are responsible for "owning the door" and authorizing access. The audit determined that an excessive number of people had access to doors. Recommendations from the report indicated a completion date of Spring 2011, and corrective actions were to include defining security manager profiles, standardizing clearance categories, [redacted] The USCP OIG conducted two audits[1] that identified the same deficiency related to prox cards. As a result, OIG decided to undertake this prox card audit.

The Security Services Bureau (SSB) is responsible for supervising and conducting security surveys of congressional offices. SSB is also responsible for storage locations containing national security information and is tasked with designing, installing, and maintaining physical security systems. SSB provides technical security countermeasure inspections and other matters ranging from the protection of data information to the protection of life and property.

[1] *Performance Audit of USCP Controls Over Evidence*, Report Number OIG-2015-03, dated February 2015; and *Performance Audit of USCP Controls Over Ammunition*, Report Number OIG-2014-03, dated March 2014.

SSB consists of three divisions: Construction Security, Physical Security, and Technical Countermeasures. Each division plays an integral part in the USCP mission. Physical Security is the SSB division charged with carrying out the security functions.

Office of Human Resources (OHR) is responsible for issuing cards when needed and collecting cards when employees terminate.

Objective, Scope, and Methodology

OIG contracted with the independent public accounting firm Cotton & Company LLP (Cotton) to conduct a performance audit of USCP prox cards. The objectives of the performance audit were to determine (1) the effectiveness of the Department's internal control over prox cards to ensure accountability of sensitive items, and (2) whether the Department complied with applicable policies and procedures, as well as applicable laws and regulations. In addition, Cotton was to follow up, if applicable, on the status of previous recommendations the House OIG made. The scope included controls, processes, and operations in place during FY 2014. Additionally, we requested and used current data related to FY 2015 when applicable.

To accomplish the objectives, we interviewed SSB officials to gain an understanding of the following:

- Structure of prox cards
- Efforts underway that address issues identified related to prox cards
- Prox card policies and procedures
- Roles and duties of personnel responsible for prox card processes and controls

We also reviewed documentation to obtain an understanding of internal controls, organizational structure, and training related to prox cards. To determine compliance, we used the following guidance:

- Draft SOP, [redacted], previously identified as [redacted] OP (Draft, since 2011)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013
- SOP 10.02, [redacted] dated August 20, 2009

For compliance with SOP [redacted], we tested a statistically sampled 45 of 166 employees

who either transferred or separated from USCP during FY 2014. As part of our testing, we compared the SSB final FY 2014 quarterly report for Department personnel, including appointed, sworn, civilian, and contractor personnel against the FY 2014 badging list the OHR badging office provided.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results

Prox cards are an important resource, and when used properly, can significantly reduce security risks. However, the controls over the prox card process have not been effective. We identified the following areas needing improvement:

- Ineffective internal controls over separated and transferred employees
- Inadequate policies and procedures
- Inadequate controls over access clearances

We did not evaluate compliance because the Department needs to finalize its policies and procedures SOP, which is still in draft format.

Ineffective Internal Controls over Separated and Transferred Employees

SOP [redacted] requires that when an employee separates from USCP, a separation checklist must be completed and returned to the Office of Human Resources (OHR). The badging office in OHR confirms that the employee returned the badge by signing off on the separation checklist. OHR must then notify SSB that the employee returned his or her badge.

When an employee transfers to another area (such as Bureau or Division) within the Department, the employee's previous security manager must review and remove the employee's prior access privileges, as applicable. The new security manager is required to add the appropriate access for the new area. In addition to adding and removing access privileges, security managers modify privileges to ensure the privileges are appropriate. To assist in carrying out that responsibility, SSB provides the security managers each quarter with *Clearance Access Definition Reports*, referred to as quarterly reports. The reports detail access clearances and doors, as well as the personnel assigned to those areas. Security managers review the report for accuracy and report for remediation any incorrect privileges to SSB.

USCP did not maintain adequate controls over prox cards for employees who separated from or transferred within the Department. We combined the transferred and separated employee

populations for FY 2014 and used the data analysis software IDEA[2] to select a random sample of 45 employees from the population of 166. In FY 2014, 103 employees separated from the Department, and 63 employees transferred within the agency. Our sample included 27 separated and 18 transferred employees.

Based on our review of final FY 2014 quarterly reports dated September 30, 2014, of the 27 employees who separated, 6 remained in the system after separating from USCP. Of those six separations, one occurred during the first quarter, four in the second quarter, none in the third quarter, and one occurred during the fourth quarter. Those totals indicate that security managers did not remove access in a timely manner. The OHR badging office collected 26 of the 27 badges except for one badge from a separated employee; SSB did remove that employee's access privileges from the [redacted] system. Guidance does not specify a timeframe for removing a separated employee from the [redacted] system.

Of the 18 employees who transferred, security managers failed to remove 17 access privileges (see Table 1). Security managers granted new access privileges for all of the transfers, and they sent an email or an access form to SSB verifying the new privileges.

Table 1 –USCP Separated and Transferred Employees During FY 2014

Separated and Transferred Employees	Total	Sample	Exceptions
Population	166	45	23
Separated	103	27	6
Transferred	63	18	17

Source: Generated from a comparison of an OHR list of *Separated and Transferred Employees* and *SSB Access Reports.*

The draft SOP entitled [redacted] states that security managers "approve, revoke, and maintain the access lists associated with all access clearances under their purview." Although the SOP has been in draft form since 2011, USCP has used it as a best practice since its creation. The SOP requires that security managers "review and validate all access lists associated with their access clearances on a quarterly basis, at a minimum." SOP [redacted] also requires that the badging office "send electronic message notification to the Security Services Bureau that the Building Access Card has been returned."

Because it is a legislative branch agency, the Department is not required to comply with SP 800-53, but sees the guidance or something similar as a best practice. NIST SP 800-53, Revision 4 provides the following guidance:

> PE-2 Physical Access Authorizations
> Control: The organization:
>
> - Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

[2] IDEA is data analysis software designed to help auditors, accountants, and other finance professionals perform data analyses quickly, to improve audits, and identify control breakdowns.

- Issues authorization credentials for facility access;
- Reviews the access list detailing authorized facility access; and
- Removes individuals from the facility access list when access is no longer required.

PS-4 Personnel Termination
Control: The organization, upon termination of individual employment:

- Terminates/revokes any authenticators/credentials associated with the individual;
- Retains access to organizational information and information systems formerly controlled by terminated individual.

PS-5 Personnel Transfer
Control: The organization:

- Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
- Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

USCP policies and procedures do not require that SSB remove access privileges for separated employees upon notification from the badging office. In addition, security managers did not thoroughly review quarterly reports to ensure that the access lists were accurate and did not remove access privileges for transferred employees when the employee transferred out of their purview.

Conclusions

Access privileges for employees who separated or had transferred are still active. Although the badging office collects prox cards at the time of an employee's separation, cards remaining active increased the risk of unauthorized use. Transferred employees continued to have access to locations for which they were no longer authorized. The quarterly reports indicate that access for some employees was not necessary. In addition, the security managers were not regularly reviewing the quarterly reports to identify discrepancies. Our review revealed that some quarterly reports contained inaccuracies and more information for the security managers to review. Unauthorized access to controlled data and physical assets created unnecessary risks as well as a vulnerability of the data or assets that the items could be destroyed or misappropriated. We therefore make the following recommendations:

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.

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

Inadequate Policies and Procedures

An authorized official, often one responsible for a Bureau or division, designates a security manager using the *Security Manager Information Form*. The security manager is responsible for monitoring and maintaining access privileges under their purview and for reviewing access privileges each quarter. SSB assists the security managers by providing quarterly reports detailing the access clearances and doors, as well as the personnel holding those access clearances. Security managers are required to review these reports and notify SSB of inaccurate information.

USCP did not maintain adequate controls related to designation and duties of security managers. As part of our review, in January 2015 we sent questionnaires to or conducted interviews with 28 security managers who performed this role during FY 2014. The length of time that each employee served as a security manager varied from 5 months to 18 years. Duration of service had little effect on the answers the security managers provided. For example, of the 28 security managers in the sampling, only 1 stated that processes had changed since becoming a security manager. The 27 remaining security managers were unaware of any changes to the processes.

Of the 28 security managers included in our review, 21 did not receive initial training on how to perform their duties. Of the 28, none of the security managers received a tutorial or SOP outlining their role (see Table 2). Only one security manager stated that he had received follow-up training.

According to the security managers, SSB did not consistently send the quarterly reports. Of the 28 security managers, 23 indicated that they received at least 1 quarterly report from SSB during FY 2014, but only 14 stated they received the reports for every quarter of FY 2014 (see Table 3). SSB stated that due to turnover of SSB staff, they were unable to locate evidence demonstrating consistent delivery of the reports. Emails that may have contained the quarterly reports could not be located due to deactivation of the email accounts when SSB staff separated from the agency.

Table 2 – Security Managers Who Received Initial Training/Tutorial

	Security Manager Responses	
	Yes	No
Provided with Initial Training	7	21
Provided with Tutorial	0	28

Source: Generated from *Security Manager Questionnaires* sent to managers in January 2015.

Table 3 – Security Managers' Receipt of Quarterly Reports from SSB

	Number of Security Managers
Not Provided with Any Quarterly Reports in FY 2014	5 out of 28
Provided with Quarterly Reports in At Least One Quarter of FY 2014	23 out of 28
Provided with Quarterly Reports in Every Quarter of FY 2014	14 out of 28

Source: Generated from *Security Manager Questionnaires* and *SSB Quarterly Reports* during FY 2015.

The [redacted] SOP states that security managers shall "approve, revoke, and maintain the access lists associated with all access clearances under their purview." Although that SOP has been in draft form since 2011, USCP has used it as a best practice since its creation. The SOP requires that security managers "review and validate all access lists associated with their access clearances on a quarterly basis, at a minimum."

Although not subject to NIST SP 800-53, we recommend that USCP use the publication or similar guidance as a best practice. NIST SP 800-53, Revision 4 provides the following guidance:

> PE-1 Physical and Environmental Protection Policy and Procedures
> Control: The organization:
>
> - Develops, documents, and disseminates:
> - Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
> - Reviews and updates the current:
> - Physical and environmental protection policy; and
> - Physical and environmental protection procedures.
>
> PE-2 Physical Access Authorizations
> Control: The organization:
>
> - Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
> - Issues authorization credentials for facility access;
> - Reviews the access list detailing authorized facility access; and
> - Removes individuals from the facility access list when access is no longer required.

SSB did not have controls to monitor or track training or guidance provided to security managers and did not provide the SOP or tutorial to the security managers designated in FY 2014. SSB did not provide updated information to security managers who held such a designation before creation of the SOP. In addition, SSB did not consistently provide quarterly reports to security managers for their review.

Conclusions

Inconsistencies existed between offices and bureaus with regard to how security managers performed their role. Security managers did not perform their duties in accordance with policies and procedures because of a lack of training and did not monitor access privileges when SSB failed to provide them with quarterly reports. Access lists could have, therefore, been inaccurate and allowed unauthorized employees to have inappropriate access privileges. Unauthorized access could have created the potential for employees to destroy or misappropriate agency assets or data.

> **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.**

> **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.**

Inadequate Controls Over Access Clearances

USCP uses prox cards to control access clearances for its personnel. Each individual receives a prox card with a unique card number. SSB enters badge numbers into the [redacted] system so that a security manager can assign access for the individual. The [redacted] system, an access security management software/hardware solution, monitors access control and monitors events. Security managers are responsible for maintaining access privileges under their control and should remove access privileges when an employee separates or transfers to an area outside their purview. To assist the security managers in carrying out this responsibility, SSB provides them with quarterly reports detailing access clearances for their review. SSB is also responsible for administering access privileges upon request of the security managers.

USCP did not maintain adequate controls over prox cards. As part of our review, we compared SSB's final FY 2014 quarterly report for all USCP personnel, including appointed, sworn, civilian, and contractor personnel (see Table 4), to the badging list for FY 2014 provided by the OHR badging office. We identified 400 individuals who had access privileges on the SSB quarterly report, but the OHR badging list did not list as having a prox card. SSB stated various circumstances could have caused this difference. Individuals who received their badges from a different agency within the Capitol Complex would not appear on the USCP OHR badging list[3];

[3] Note: In addition to USCP employees, contractors receiving USCP badges would also be included on the OHR badging list.

however, they may still have access to USCP controlled areas. In these instances, the security manager of the USCP area must complete the SSB access form to grant access to this individual. Names SSB deactivated in the [redacted] system within the last two years are still included on the SSB quarterly report but would no longer remain on the OHR badging list. Due to recordkeeping requirements pertaining to SSB, the Department must maintain an individual's access records for two years. Unless the security managers request that SSB remove individuals from the *Clearance Access Definition Reports*, the names will continue to appear each quarter with clearances, although SSB deactivated the prox card. SSB confirmed there were exceptions related to the 400 individuals, but they were unable to quantify the errors until confirming with the appropriate security managers.

We found 73 instances in which an individual was included on both lists, but had a different badge number in each list (see Table 5). SSB stated that various circumstances could have caused these instances. Agencies within the Capitol Complex have begun using dual-token smartcards for certain individuals. These cards contain a radio frequency identification (RFID) chip and a token similar to those used in traditional prox cards. Unlike the traditional prox cards used by most of USCP, the number on the smartcard refers to the RFID. OHR has no way of reading the prox card number, and therefore records the 5 digit RFID number for these cards. SSB records the prox card number in their system to grant the individual access to their assigned clearances. Number transposition and entering extra numbers could also create differences between the two lists. SSB stated that the prox card numbers in the [redacted] system must be accurate for the individual to have access to their assigned clearances.

In addition, there were instances where individuals in the [redacted] system did not have an Employing Office/Company listed. In these instances, SSB listed the office as "blank."

Table 4 – Classification of Individuals from OHR

Classification
Appointed
Sworn
Civilian
Contractor

Source: Generated from *OHR Badging List* for FY 2014.

Table 5 – Summary of Differences Related to Access Clearances

Category	Number of Employees
SSB Listing Total	2,485
Individuals Not on Badging List	400
Individuals with Differing Badge Numbers	73

Source: Generated from comparing *Access Clearance Definition Reports* to the *OHR Badging List* for FY 2014.

The Department drafted and has used the [redacted] SOP as a best practice prior to FY 2014,which states that security managers "approve, revoke, and maintain the access lists associated with all access clearances under their purview." The SOP also states that security managers shall "review and validate all access lists associated with their access clearances on a quarterly basis, at a minimum."

Although USCP is not subject to NIST SP 800-53, Revision 4, we recommend that USCP use that publication or similar guidance as a best practice. NIST SP 800-53, Revision 4 provides the following guidance:

> PE-2 Physical Access Authorizations
> Control: The organization:
>
> - Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
> - Issues authorization credentials for facility access;
> - Reviews the access list detailing authorized facility access; and
> - Removes individuals from the facility access list when access is no longer required.

SSB did not consistently send quarterly reports to all security managers for review. Security managers did not provide complete and accurate information to SSB when granting new access privileges. In addition, security managers did not thoroughly review the quarterly reports for accuracy.

Conclusions

Because SSB and OHR data were not consistent, validation was not possible. Inconsistencies made comparison of OHR listings to SSB access lists time consuming and yielded little value. Using data with consistent naming conventions would enable verification that security managers were adhering to their responsibilities. In all instances, security managers should provide information related to the "Employing Office/Company" field when they request access privileges for individuals who received their badge from USCP or any other agency. In addition, individuals who no longer needed access privileges continued to have access without a valid prox card, resulting in the potential for inappropriate access. Unauthorized access created a potential for employees to destroy or misappropriate agency assets or data.

> **<u>Recommendation 5</u>: 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.**

APPENDICES

Listing of Recommendations

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.

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

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.

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.

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.

Department Comments

UNITED STATES CAPITOL POLICE
OFFICE OF THE CHIEF
119 D STREET, NE
WASHINGTON, DC 20510-7218

March 27, 2015

COP 150394

MEMORANDUM

TO: Ms. Fay F. Ropella, CPA,CFE
Inspector General

FROM: Kim C. Dine
Chief of Police

SUBJECT: Response to Office of Inspector General (OIG) draft report *Performance Audit of USCP Proximity (Prox) Cards* (Report No. OIG-2015-05).

The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of the Inspector General's (OIG's) draft report *Performance Audit of USCP Proximity (Prox) Cards* (Report No. OIG-2015-05).

The Department 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 Prox 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 men and women of the United States Capitol Police is appreciated.

Very respectfully,

Kim C. Dine
Chief of Police

cc: Daniel Malloy, Assistant Chief of Police
[redacted] USCP Audit Liaison
Mr. Robert Ford, Security Services Bureau

NOTES

This page intentionally left blank

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 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
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL