UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Analysis of the
United States Capitol Police
Insider Threat Detection Program

Report Number OIG-2017-08

June 2017

~~REPORT RESTRICTION LANGUAGE~~

~~Distribution of this Document is Restricted~~

~~This report contains sensitive law enforcement material and is the property of the Office of the 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.~~

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. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG and discussed the draft 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

TABLE OF CONTENTS

	Page
Abbreviations and Acronyms	iii
Executive Summary	1
Background	2
Objectives, Scope, and Methodology	3
Results	4
Improvements to Controls Needed	4
Appendices	8
Appendix A – List of Recommendations	9
Appendix B – Department Comments	10

Abbreviations and Acronyms

Code of Federal Regulations	CFR
[redacted]	[redacted]
Fiscal Year	FY
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
National Institute of Standards and Technology	NIST
Personally Identifiable Information	PII
Special Access Program	SAP
Sensitive Compartmented Information	SCI
Special Publication	SP
Standard Operating Procedure	SOP
United States Capitol Police	USCP or the Department

[redacted]

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) administers USCP's Insider Threat Detection Program. According to the Department of Homeland Security, "An insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems." The OIS Security Division administers elements of the program; however, insider threat detection and prevention is an entity wide endeavor.

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of the USCP Insider Threat Detection Program. The objective of our analysis was to determine how effectively the Department protects its information systems, which contain National Security Information and Law Enforcement Sensitive data, from threats posed by employees, especially those with special or elevated access to unclassified information technology systems or information based on their job description function.

The scope of the analysis included evaluation of controls, processes, and operations from October 1, 2015, through March 31, 2017. In certain instances, we analyzed data produced after March 31, 2017, which was the most recently available information.

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Control PM-12 identifies the elements of an insider threat program. Typically, a comprehensive program consists of a detailed policy; a rigorous repeatable process for investigating insider threat alerts and incidents, timely removal of network access for separated employees; and a robust background investigation process for newly hired employees.

The Department used elements of its insider threat program, such as automated tools, to alert OIS personnel of potential insider threats. It also required annual security awareness training to educate employees about threats, and notified employees about real-time issues by sending Department-wide emails about incidents.

USCP did not; however, have a comprehensive program for including an overall plan that established policy and assigned responsibilities for its insider threat program—which would have established a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. In addition, OIS did not have a rigorous repeatable process for investigating insider threat alerts and incidents as required by best practices. Without an insider threat policy and a repeatable process of following up on alerts, the Department may overlook or not properly respond to incidents resulting in potentially exposing sensitive law enforcement information and congressional data.

Of the 164 employees separating from the Department between October 1, 2015, and March 31, 2017, 4 still had active network accounts. For example, one employee who separated from the Department on January 6, 2017, still had an active network account as of April 24, 2017. Such a condition is a reoccurring audit finding, first identified in the audit of the Fiscal Year (FY) 2007 financial statements and closed in the FY 2008 financial statement audit. Unattended or unmonitored accounts pose a serious risk to the Department because exiting or disgruntled employees could maintain access to the USCP network, possibly enabling unauthorized and unmonitored access from an outside third party.

USCP also had an outdated policy about background investigations for newly hired employees. Standard Operating Procedure (SOP) [redacted], dated July 25, 2001, was not up to date because it reflects an organizational unit that no longer exists as responsible for performing background investigations. Additionally, the Department does not require that employees and contractors with special or elevated access to USCP networks obtain a security clearance as best practices suggest.

On March 23, 2017, prior to the start of our work, OIS conducted a briefing with the Chief of Police related to cyber issues, and acknowledged risks and issues related to insider threat. OIG recommends that the Department continue its efforts to establish a comprehensive plan for addressing insider threat controls, processes, and operations. See Appendix A for a complete list of OIG recommendations.

On June 19, 2017, OIG conducted an exit conference and on June 7, 2017, we provided a draft report to Department officials. We incorporated the Department's comments as applicable and attached their response to the report in its entirety in Appendix B.

Background

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control PM-12, provides guidance on establishing an insider threat program that complies with the requirements and minimum standards for preventing, deterring, detecting, and mitigating actions by malicious insiders. According to the Department of Homeland Security, "An insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems." Insider threats can include harm to contractor or program information to such an extent that the information impacts the contractor or Department obligations to protect national security or law enforcement information.

The Office of Information Systems (OIS) Security Division is responsible for the Insider Threat Detection Program within the United States Capitol Police (USCP or the Department). OIS used various tools for identifying potential threat incidents. For example, OIS used annual security

awareness training to educate Department employees about potential threat issues and effective ways of spotting insider threat incidents.

Standard Operating Procedure (SOP) [redacted], dated July 25, 2001, assigns responsibility for performing background investigations.

OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of USCP's Insider Threat Detection Program. The objective of the analysis was to determine how effectively the Department protects its information systems and data from threats posed by employees, especially those with special or elevated access to unclassified information technology systems or information based on their job description function. The scope of the analysis included controls, processes, and operations beginning in Fiscal Year (FY) 2016 and ending March 31, 2017. In certain instances, we analyzed data produced after March 31, 2017, because it was the most recently available information.

To accomplish our objectives, we interviewed relevant Department officials to gain an understanding of the following areas:

- Nature of the current insider threat detection program
- Controls related to the insider threat detection program
- Tools OIS uses for monitoring network activity for potential insider threats
- Nature of the current annual security awareness training
- Previous incidents of insider threats

To understand backup and recovery capabilities, we reviewed the following guidance:

- USCP Directive [redacted], dated April 27, 2017
- USCP Directive [redacted], dated April 26, 2017
- USCP Directive [redacted], dated April 21, 2017.
- USCP Directive [redacted], dated April 21, 2017
- USCP Directive [redacted], dated October 29, 2015

- USCP SOP [redacted], dated July 25, 2001

We also used NIST guidance. As a legislative branch entity, many laws and regulations that apply to executive branch agencies do not apply to USCP. We believe, however, that those laws and regulations not only represent effective guidance but are also best practices for USCP.

OIG conducted this analysis in Washington, D.C., from April through May 2017. We did not conduct an audit, the objective of which would be the expression of an opinion on Department programs. Accordingly, we do not express such an opinion. OIG did not conduct this analysis in accordance with generally accepted government auditing standards. Had we conducted an audit and followed such standards, other matters might have come to our attention. We conducted an exit conference on June 19, 2017. We provided a draft copy of this report to Department officials for comment on June 7, 2017. We incorporated Department comments as applicable and attached their response to the report in its entirety as Appendix B. ~~This report is intended solely for the information and use of the Department, the United States Capitol Police Board, and USCP Oversight Committees and should not be used by anyone other than the specified parties.~~

RESULTS

The Department should improve its controls over insider threat detection. Improving controls should help create a more effective program and would include actions such as updating and aligning Department policies and procedures.

Improvements to Controls Needed

The Department should continue efforts toward improving its threat detection program for insiders. For example, USCP did not have a program policy for internal threats or have a rigorous repeatable process for identifying and investigating potential insider threat incidents. OIS also did not always deactivate network accounts for terminating employees in a timely manner. Finally, USCP's policy regarding background investigations for new employees was not up to date and placed the responsibility for background investigations on an organizational unit that no longer exists.

Lack of a Program Policy for Insider Threat Detection

The Department did not have an entity-wide policy for insider threat detection. According to OIS personnel, the Department handles insider threat incidents via the incident management process but without dedicated personnel. On March 23, 2017, prior to the start of our work, OIS conducted a briefing with the Chief of Police related to cyber issues, and acknowledged risks and issues related to insider threat.

NIST SP 800-53, Revision 4, Control PM-12 states, "The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team." Without a comprehensive policy, management does not have an effective way of properly correlating

Department resources in the event of an insider threat. While many elements of an insider threat detection program would fall under the purview of OIS, insider threat should be a Department-wide effort.

Incident Response Monitoring and Responding

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control IR-4 states, "The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery." Because it did not have a comprehensive insider threat policy, the Department was not able to maintain a rigorous repeatable process for responding to and investigating threat alerts and incidents. According to officials, each day OIS receives as many as 100 alerts of potential insider threat activity on its network. Because the process for investigating alerts is left to individuals receiving such alerts, legitimate insider threat incidents could go undetected.

[redacted]

Network Access for Separated Employees

OIS did not disable network accounts for separated employees within 24 hours of separation as required by USCP Directive [redacted] dated April 21, 2017. Of the 164 employees separated from the Department between October 1, 2015, and March 31, 2017, 4 continued to have active network accounts during our review. For example, one employee separated from the Department on January 6, 2017, still had an active network account on April 24, 2017.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Control AC-2 states, "the Organization: g. Notifies account managers: When users are terminated or transferred . . ." According to officials, the Office of Human Resources (OHR) or employee's office of record did not request that OIS disable the accounts. However, separation checklists for the four employees show that OIS reviewed and signed the checklists certifying that OIS removed "PC Access" and "Email Account" on or before the dates, the employees separated.

Unattended or unmonitored accounts pose a risk to the Department because exiting or disgruntled employees could present the account information to an acquaintance or third party. As a result, the acquaintance or third party could easily gain access to the USCP network—making network information vulnerable. Although OIG previously reported the issue in 2007 and closed the recommendation in an audit of the FY 2008 financial statements, the condition indicates a pattern of inadequate controls and monitoring for ensuring disabling of accounts for separated employees. Prior to the issuance of our report, OIS removed the network access for these employees.

Outdated Background Investigation Policy

USCP Directive [redacted], dated October 29, 2015, assigns Bureau Commanders and Office Directors the responsibility of "ensuring respective Directives and SOPs are updated, as needed, and reviewed annually." However, SOP [redacted], dated July 25, 2001, was out of date because it placed the responsibility for performing background investigations for new employees on an organizational unit that no longer exists. In addition, the copy of the SOP found on PoliceNet[1] was missing page two. On June 13, 2017, the USCP Audit Liaison provided the OIG with page 2 of the SOP and had PoliceNet updated to reflect the missing page.

Lack of Security Clearances

USCP has not determined which Department-wide systems or sensitive data pose an elevated insider threat risk, and the Department did not require employees or contractors with access to these systems or data to obtain a security clearance or recurring background checks based on their job description function. Although not applicable to the legislative branch, best practices

[1] PoliceNet is the Department's internal webpage where copies of policies are available for employees to access.

such as the Code of Federal Regulations (CFR), 5 CFR § 1400.201 require that the following sensitive positions obtain additional pre-appointment investigations:

1. Noncritical-Sensitive positions are national security positions which have the potential to cause significant or serious damage to the national security

2. Critical-Sensitive positions are national security positions which have the potential to cause exceptionally grave damage to the national security

3. Special-Sensitive positions are those national security positions which have the potential to cause inestimable damage to the national security, including but not limited to positions requiring eligibility for access to Sensitive Compartmented Information (SCI), requiring eligibility for access to any other intelligence-related Special Sensitive information, requiring involvement in Top Secret Special Access Programs (SAP), or positions which the agency head determines must be designated higher than Critical-Sensitive consistent with Executive order.

Conclusions

Although it had elements of an insider threat program, the Department did not have a comprehensive program. The Department should make improvements in controls for an effective insider threat program by updating policies and procedures that would align with the NIST framework and strategic plans as well as provide visibility and automatic remediation. OIG, therefore, makes the following recommendations.

Recommendation 1: We recommend that the United States Capitol Police develop and implement a Department-wide policy related to insider threat detection that aligns with the National Institute of Standards and Technology framework and strategic plans.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems develop and implement a documented assessment and prioritization process specific to insider threat to identify, analyze, and report on insider threat events.

Recommendation 3: We recommend that the United States Capitol Police fully implement its controls to ensure that the Office of Information Systems disable accounts for terminated employees in a timely manner (for example, 24 hours).

Recommendation 4: We recommend that the United Stated Capitol Police update Standard Operating Procedure [redacted], dated July 25, 2001, to reflect changes in the background investigation process.

Recommendation 5: We recommend that the United States Capitol Police (USCP or the Department) determine which systems pose an elevated insider threat risk. Additionally, USCP should consider requiring employees and contractors with access to these systems to obtain a security clearance or recurring background checks to ensure that these individuals do not pose a significant risk to the network

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police develop and implement a Department-wide policy related to insider threat detection that aligns with the National Institute of Standards and Technology framework and strategic plans.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems develop and implement a documented assessment and prioritization process specific to insider threat to identify, analyze, and report on insider threat events.

Recommendation 3: We recommend that the United States Capitol Police fully implement its controls to ensure that the Office of Information Systems disable accounts for terminated employees in a timely manner (for example, 24 hours).

Recommendation 4: We recommend that the United Stated Capitol Police update Standard Operating Procedure [redacted], dated July 25, 2001, to reflect changes in the background investigation process.

Recommendation 5: We recommend that the United States Capitol Police (USCP or the Department) determine which systems pose an elevated insider threat risk. Additionally, USCP should consider requiring employees and contractors with access to these systems to obtain a security clearance or recurring background checks to ensure that these individuals do not pose a significant risk to the network.

[redacted]

DEPARTMENT COMMENTS

Phone: 202-224-9800

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

June 21, 2017

COP 170448

MEMORANDUM

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

FROM: Matthew R. Verderosa
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Analysis of the United States Capitol Police Insider Threat Detection Program* (Report No. OIG-2017-08)

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 *Analysis of the United States Capitol Police Insider Threat Detection Program* (Report No. OIG-2017-08).

The Department generally agrees with all of the recommendations and appreciates the opportunity to further improve upon the policies and procedures within the Office of Information Systems. The Department will assign Action Plans to appropriate personnel regarding each recommendation to achieve long-term resolution of each matter.

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

CONTACTING THE OFFICE OF INSPECTOR GENERAL

Success of the OIG mission to prevent fraud, waste, abuse, or mismanagement depends on the cooperation of employees and the public. There are several ways to report questionable activity.

Call us at 202-593-3868 or toll-free at 866-906-2446. A confidential or anonymous message can be left 24 hours a day/7 days a week.

Toll-Free - 1-866-906-2446

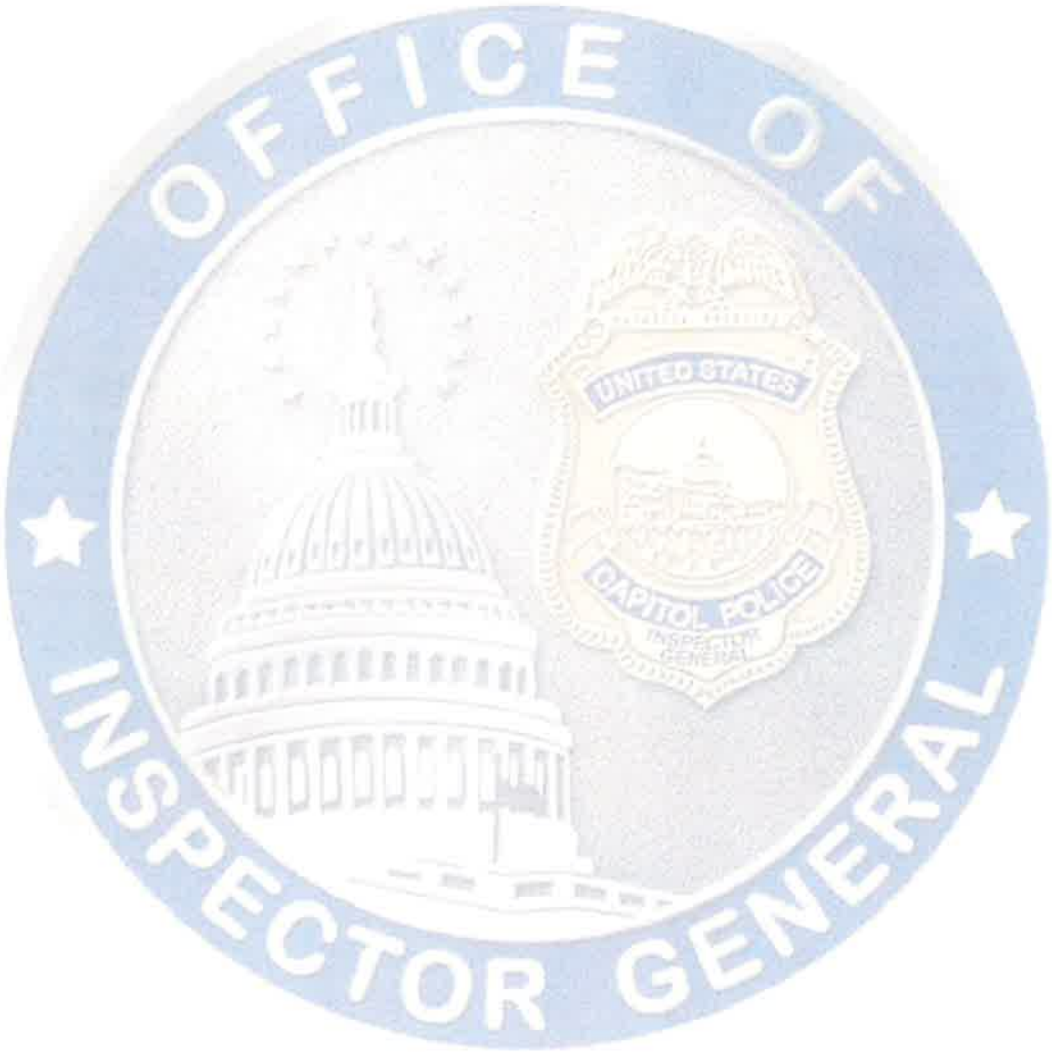
Write us:
United States Capitol Police
Attn: Office of Inspector General
499 South Capitol St. SW, Suite 345
Washington, DC 20003

Or visit us:
499 South Capitol Street, SW, Suite 345
Washington, DC 20003

You can also contact us by email at: OIG@USCP.GOV

When making a report, convey as much information as possible such as:
Who? What? Where? When? Why? Complaints may be made anonymously or you may request confidentiality.

Additional Information and Copies:
To obtain additional copies of this report, call OIG at 202-593-4201.


OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL