UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Analysis of the
United States Capitol Police
Email Security

Report Number OIG-2019-06

March 2019

~~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.~~

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 in 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.

Michael A. Bolton
Inspector General

TABLE OF CONTENTS

Abbreviations and Acronyms	iii
Executive Summary	1
Background	2
Objectives, Scope, and Methodology	2
Results	4
Improvements to Controls Needed	4
Appendices	6
Appendix A – Recommendations	7
Appendix B – Department Comments	8

Abbreviations and Acronyms

Binding Operational Directive	BOD
Department of Homeland Security	DHS
National Institute of Standards and Technology	NIST
Office of Information Systems	OIS
Office of Inspector General	OIG
Special Publication	SP
Storage Area Network	SAN
United States Capitol Police	USCP or Department

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) administers the email security program for the Department. USCP operates its email system on email servers located at the Department's primary and backup data centers. OIS performs the security configuration and is responsible for controls over email services as well as storing emails on the Storage Area Network (SAN). A SAN is an array of storage devices working in unison to store data and capable of replicating between one or more SAN arrays.

To address challenges noted in our report titled *Top Management Challenges Facing the United States Capitol Police*, dated October 2018, the Office of Inspector General (OIG) conducted an analysis of the USCP email security program. The objectives of our analysis were to determine if the Department (1) established adequate internal controls and processes for ensuring security over the Department's email system, and (2) complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. Our scope included controls, processes, and operations during Fiscal Year 2018.

Overall, the Department could improve its internal controls related to email security. For example, the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security*, dated October 16, 2017, requires that Federal agencies activate increased email security by [redacted] on their network. [redacted] As a legislative branch agency, USCP is not required to comply with the DHS BODs; however, we believe that the recommendations in the directive serve as best practices. As of March 4, 2019, USCP had not implemented [redacted]

National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013, control CM-2 states, "the organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system." However, [redacted]

To improve email security controls, OIG made three recommendations detailed in Appendix A. On March 7, 2019, 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

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) administers the email security program for the Department. Email security comprises mail servers and applications operated out of both a primary and backup data center. Both data centers replicate workloads to ensure email services are available and delivered timely to the USCP workforce.

OIS performs the security configuration and controls over the email services. Emails entering or exiting the USCP environment must pass through a [redacted][1] firewall that uses rulesets to either allow or deny emails. Emails that do not meet the allowed rulesets are blocked and denied entry to the USCP environment. Microsoft Exchange[2] email servers located within the USCP environment are managed by OIS and are used to disseminate email to local USCP Outlook and USCP iPhone users.

USCP maintains storage of emails on its Storage Area Network (SAN)[3] located at both the primary and backup data centers. [redacted]

OBJECTIVES, SCOPE, AND METHODOLOGY

To address challenges noted in our report titled *Top Management Challenges Facing the United States Capitol Police*, dated October 2018, the Office of Inspector General (OIG) conducted an analysis of the USCP email security program. The objectives of our analysis were to determine if the Department (1) established adequate internal controls and processes for ensuring security over the Department's email system, and (2) complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. Our scope included controls, processes, and operations during Fiscal Year 2018.

To accomplish our objectives, we interviewed Department officials to gain an understanding of the email security program. We also reviewed the following guidance related to email security:

- USCP Directive [redacted] dated January 9, 2019
- USCP Directive [redacted] dated January 9, 2019

[1] [redacted] is a boundary protection system used to apply rulesets to all incoming and outgoing internet traffic for the USCP Network.
[2] Microsoft Exchange is the USCP email service, which communicates and receives all USCP emails.
[3] An SAN is an array of storage devices working in unison to store data and capable of replicating between one or more SAN arrays.

[redacted]

- USCP Directive [redacted] dated January 9, 2018
- Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security*, dated October 16, 2017
- USCP Directive [redacted] dated April 21, 2017
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-177, *Trustworthy Email*, dated September 2016
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013
- NIST SP 800-45 Version 2, *Guidelines on Electronic Mail Security*, dated February 2007
- USCP [redacted] dated February 18, 2005

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 represent appropriate guidance and industry best practices for USCP.

To assess the effectiveness of controls, OIG reviewed policies and procedures to determine if the Department handled malicious emails appropriately, had an adequate encryption policy, and had proper physical security of email infrastructure. To assess compliance with policies and procedures as well as applicable laws, regulations, and best practices, we reviewed the Department's policies and procedures related to email security. We also reviewed various best practices such as guidance from NIST.

OIG conducted this analysis in Washington, D.C., from September 2018 through February 2019. 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 provided a draft copy of this report to Department officials for comment on March 7, 2019. A list of recommendations is detailed in Appendix A. We incorporated Department comments as applicable and attached its response to the report in its entirety as Appendix B. ~~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

Overall, USCP did not implement some internal controls that could have improved the security of the Department's email system. Without proper internal controls, USCP ran the risk of third parties reading outbound emails in transit and possibly and unknowingly using servers with compromised settings.

Improvements to Controls Needed

The Department could improve its internal controls by implementing security functions noted in the DHS guidance. Additionally, the Department could improve its internal controls by implementing an organizationally defined baseline for email servers.

Email Security Implementation of Security Functions

USCP did not implement the best practices identified in DHS BOD 18-01. DHS BOD 18-01 requires that Federal agencies activate increased email security. According to the BOD, agencies should [redacted] on their networks. [redacted]

Email Server Configuration

The Department configured its Microsoft Exchange email servers without defined baselines prior to utilizing the servers. Additionally, the mail servers were not subject to review for baseline compliance to ensure that operational mail servers do not have altered configurations.

NIST SP 800-53, Revision 4, control CM-2 states, "the organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system." Additionally, control CM-6 of NIST SP 800-53 states that the organization "monitors and controls changes to the configuration settings in accordance with organizational policies and procedures."

[redacted]

[redacted]

Conclusions

Although not required to follow either DHS BODs or NIST guidance, USCP could improve its controls by following the best practices. OIG, therefore, makes the following recommendations:

Recommendation 1: We recommend that the United States Capitol Police Office of Information Systems consider [redacted] for Microsoft Exchange mail servers.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems implement organizationally defined baselines for Microsoft Exchange mail servers.

Recommendation 3: We recommend that the United States Capitol Police Office of Information Systems implement baseline configurations scans for all Microsoft Exchange mail servers.

APPENDICES

List of Recommendations

Recommendation 1: **We recommend that the United States Capitol Police Office of Information Systems consider [redacted] for Microsoft Exchange mail servers.**

Recommendation 2: **We recommend that the United States Capitol Police Office of Information Systems implement organizationally defined baselines for Microsoft Exchange mail servers.**

Recommendation 3: **We recommend that the United States Capitol Police Office of Information Systems implement baseline configurations scans for all Microsoft Exchange mail servers.**

DEPARTMENT COMMENTS

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

March 20, 2019

COP 181325

MEMORANDUM

TO: Mr. Michael A. Bolton
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 Email Security* (Report No. OIG-2019-06)

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 Email Security* (Report No. OIG-2019-06).

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 within the Department. 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.

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 202-593-1972 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

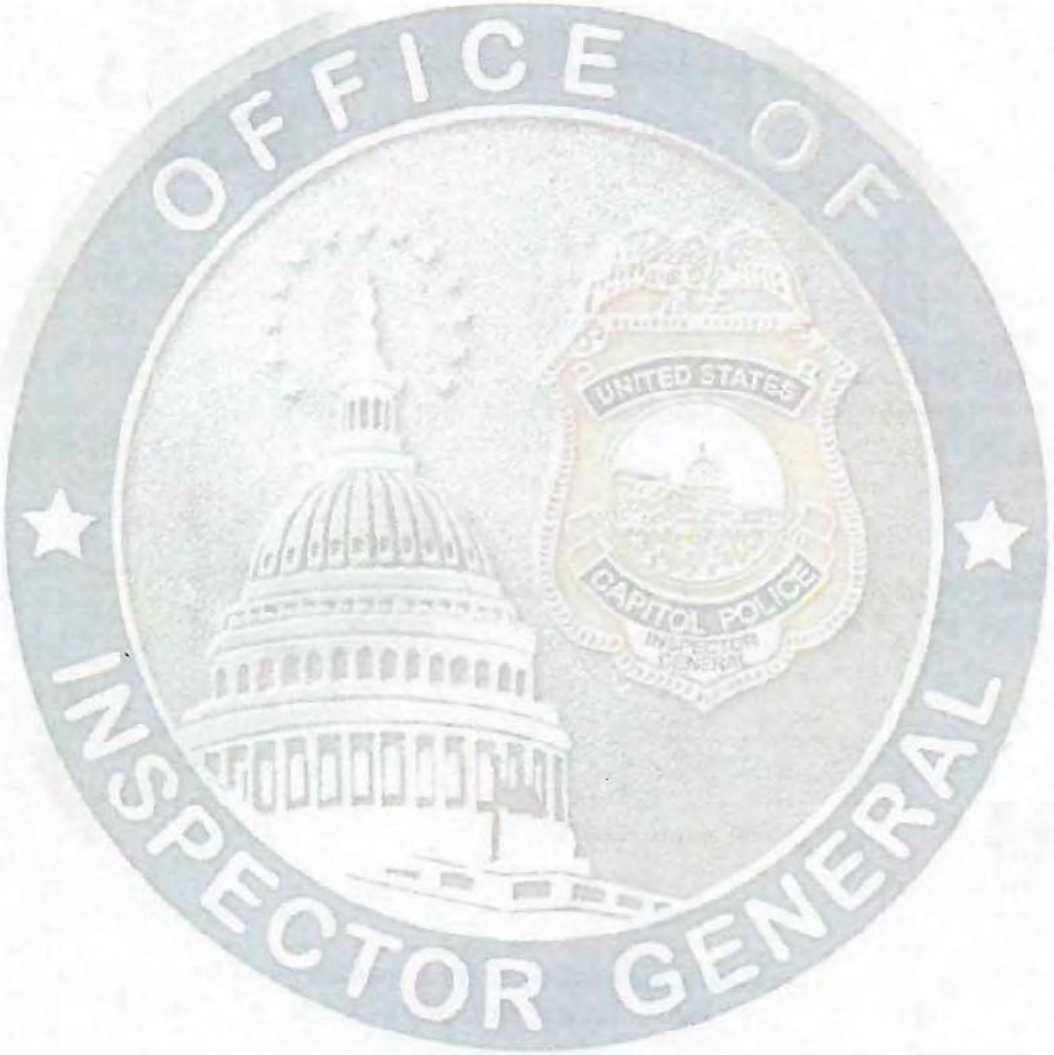
Or visit us:
499 South Capitol Street, SW, Suite 345
Washington, DC 20003

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