

# UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL

## Analysis of the United States Capitol Police Monitoring of Internet Usage for Waste and Abuse Report Number OIG-2018-09 March 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.~~





## *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 analysis 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, CPA, CFE  
Inspector General

**This page intentionally left blank**

## TABLE OF CONTENTS

	<u>Page</u>
Abbreviations and Acronyms	iii
Executive Summary	1
Background	2
Objectives, Scope, and Methodology	3
Results	4
Monitoring Internet Usage	4
Identifying and Responding to Waste and Abuse	7
Appendices	9
Appendix A – List of Recommendations	10
Appendix B – Department Comments	11

## Abbreviations and Acronyms

Fiscal Year	FY
National Institute of Standards and Technology	NIST
Office of Inspector General	OIG
Office of Information Systems	OIS
Security Information and Event Management	SIEM
	
United States Capitol Police	USCP or the Department
Universal Resource Locator	URL

---

## EXECUTIVE SUMMARY

---

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) monitors internet and network traffic for the Department. The primary function of the internet monitoring at USCP is to identify and respond to malicious traffic.

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of the Department's internet usage and monitoring capabilities. The objectives of the analysis were to determine if the Department possessed (1) the capability for monitoring internet usage, and (2) the ability to identify, and respond to, potential waste or abuse. Our scope included controls, processes, and operations during Fiscal Year (FY) 2017. In certain instances, we analyzed data from FY 2018 because OIS monitoring tools contained only a limited amount of historical information.

While the Department had tools in place for monitoring, capturing, and reviewing internet usage and activities across the USCP network, opportunities exist for enhancing capabilities. For example, the Department [REDACTED]

[REDACTED]. On February 13, 2018, the Director of National Intelligence testified before the U.S. Senate Select Committee on Intelligence and stated "Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year."<sup>1</sup> Information reviewed showed that [REDACTED] hosted a significant portion of the [REDACTED] by USCP systems. [REDACTED] increases the risk of end-users visiting malicious sites known to distribute malware.

The monitoring tools also did not always capture complete activity. Of the 5 days examined, 4 days of aggregated information did not capture multiple hours of missing activity across the sampled days. Failure to capture complete activity to a centralized location decreases the ability of an organization to correlate across differing repositories for situational awareness throughout organizations. Additionally, missing data increases the risk of wasteful and abusive activity going undetected, uninvestigated, and unresolved. OIS provided data for an additional three days during February 2018. There was no missing data in the additional three days that we reviewed. As a result, OIG will not make a recommendation regarding this issue. However, OIS should continue to monitor this issue to ensure monitoring tools are capturing complete data.

USCP Directive [REDACTED], states that the Department permits *de minimis*<sup>2</sup> use of resources for personal use when "such uses are performed without measurable interference to the performance of the official duties." The Directive does not define "measurable interference" or identify internet activities deemed

---

<sup>1</sup> *Worldwide Threat Assessment of the U.S. Intelligence Community*.

(<https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.)

<sup>2</sup> *De minimis* is a Latin phrase commonly understood to mean "so minor as to merit disregard."

counterproductive or negatively affecting an employee's productivity. The Department also did not actively monitor USCP employee and contractor internet activity for waste or abuse. Because it primarily monitors internet traffic for malicious activity, OIS did not fully incorporate methods of internet use monitoring that would identify waste or abuse.

To develop more efficient and effective controls over monitoring internet traffic for waste and abuse, the Department should enhance its monitoring network capabilities and formally define measurable interference to ensure personnel are aware of what constitutes waste and abuse. See Appendix A for a complete list of OIG recommendations.

On March 19, 2018, OIG conducted an exit conference. On March 7, 2018, 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) monitors internet activity across the Department using various tools. USCP operated the tools from the primary and backup data center, which capture individual usage, systems,<sup>3</sup> and connections across the USCP network and to the internet.

In early Fiscal Year (FY) 2018, OIS implemented a new software tool for Security Information and Event Management (SIEM) from [REDACTED]. The introduction of [REDACTED] gave the Department increased capabilities for capturing, tracking, and monitoring activity at USCP. Before [REDACTED], the Department used [REDACTED] as its SIEM tool. The change in SIEM tools was the result of a need for increased capabilities.

The Department uses [REDACTED] to aggregate, analyze, and consolidate log data from multiple monitoring tools and applications. [REDACTED] provides firewall and security endpoint tools and monitors inbound and outbound internet traffic at USCP. [REDACTED] captures information logs from [REDACTED] and creates dashboards based on the information. The dashboards provide useful information about internet traffic and include activity use based on criteria, such as suspicious or malicious sites visited, and trends across a timeframe.

Aggregated information captured through [REDACTED] from tools such as [REDACTED] allow for aggregated monitoring of USCP web traffic. One key use of the information is incident response. OIS receives notifications of incidents by system tools through alerts or emails generated by [REDACTED]. OIS also receives requests from supervisors to assist in determining whether internet traffic constitutes waste or abuse.

---

<sup>3</sup> Including desktops, workstations, servers, tablets, and mobile devices on the USCP network.

## OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of the Department's internet usage and monitoring capabilities. The objectives of the analysis were to determine if the Department possessed (1) the capability of monitoring internet usage, and (2) an ability to identify, and respond to, potential waste or abuse. Our scope included controls, processes, and operations during FY 2017. In certain instances, we analyzed data from FY 2018 because OIS monitoring tools contained only a limited amount of historical information.

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

- USCP system tools for monitoring internet traffic and activity
- Policies and procedures for incident response
- System configurations on the external boundaries of the USCP network
- Internet usage policies for the Department
- Nature of USCP's internet traffic

We also reviewed the following guidance:

- USCP Directive [REDACTED], dated January 24, 2018
- USCP Directive [REDACTED], dated April 27, 2017
- USCP Directive [REDACTED]  
[REDACTED] dated August 4, 2015
- USCP Directive [REDACTED], dated February 19, 2015

We also used National Institute of Standards and Technology (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.

We randomly selected a sample of log data from the [REDACTED] SIEM tool for 5 days in early FY 2018 (October 17 and 23, 2017; November 10, 2017; December 4, and 12, 2017.) We selected those dates from FY 2018 rather than during FY 2017 because certain monitoring tools could only maintain a limited amount of historical information.

OIG conducted this analysis in Washington, D.C., from September 2017 through February 2018. 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 March 19, 2018 and provided a draft copy of this report to Department officials for comment on March 7, 2018. See Appendix A for a complete list of recommendations. 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 USCP Board, and USCP Oversight Committees and should not be used by anyone other than the specified parties.

## RESULTS

The Department has opportunities that should enhance its capabilities for monitoring internet usage. Additionally, the Department should more clearly define internet usage that constitutes waste and abuse.

### Monitoring Internet Usage

The Department did not configure its monitoring tools used for [REDACTED] known to have an elevated cybersecurity threat. Additionally, the Department's monitoring tools it did have were not always actively monitoring internet traffic.

### Monitoring Tool Configuration

[REDACTED]. The Department implemented use of [REDACTED] in early FY 2018. That SIEM tool captures log data from various monitoring applications at the Department. [REDACTED], the primary firewall and endpoint security application on the network, sends aggregated logs to [REDACTED] about internet activity by USCP systems and individuals.

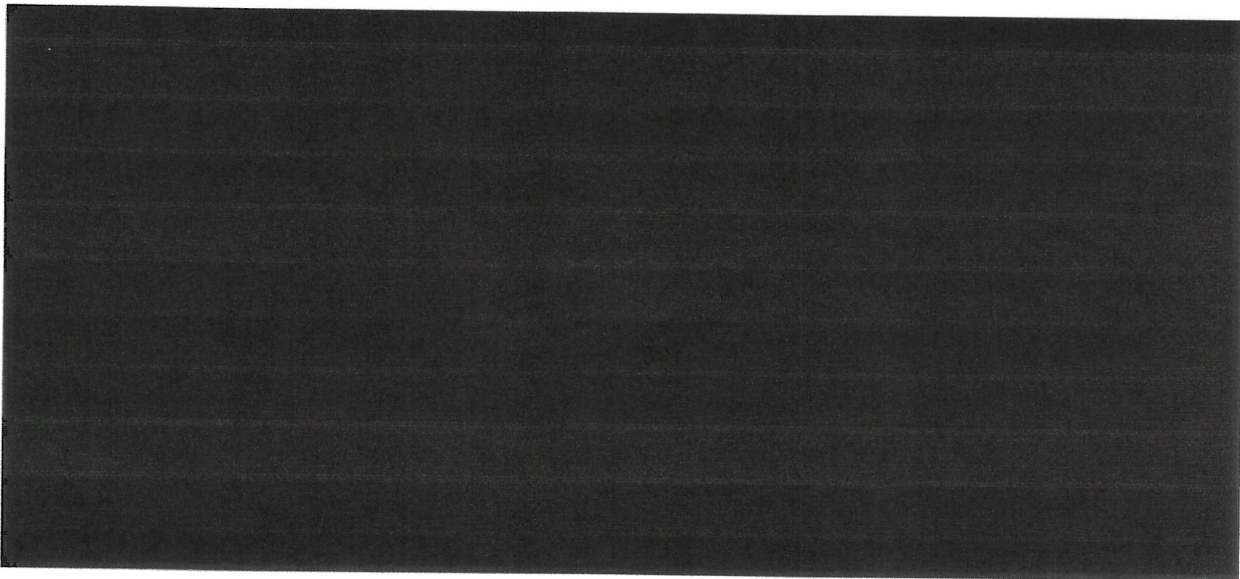
NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control SC-7 states the organization should establish and review policies for restricting traffic flows no longer supported by an explicit mission or business need.

Web traffic from [REDACTED] constitutes an enhanced cybersecurity threat. On February 13, 2018, the Director of National Intelligence, testified before the U.S. Senate Select Committee on Intelligence and stated, "Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year."<sup>4</sup> Information from OIS showed

<sup>4</sup> *Worldwide Threat Assessment of the US Intelligence Community*.  
(<https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>)

that [REDACTED] had hosted a significant portion of the [REDACTED] by USCP systems. [REDACTED] increases the risk of end-users visiting malicious sites known to distribute malware.

OIS officials stated that for functionality purposes USCP [REDACTED] [REDACTED] in order to grant access to specific Uniform Resource Locators (URLs) and websites under those domains. [REDACTED]



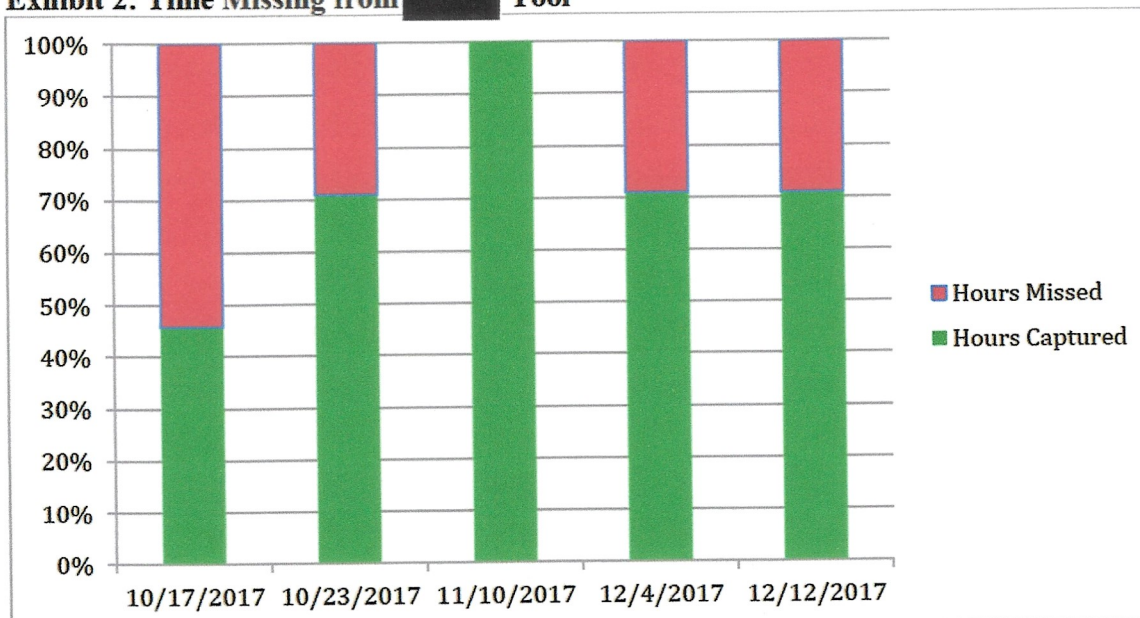
### Monitoring Tool Data Capture

[REDACTED] operates as a firewall and security endpoint tool and monitors inbound and outbound internet traffic at USCP. [REDACTED] sends log data to the [REDACTED] SIEM tool and to [REDACTED], the legacy SIEM. We examined [REDACTED] log data using a sample of 5 days<sup>5</sup> based on information from [REDACTED]. Of the 5 days examined, [REDACTED] had not aggregated information for several hours across 4 of the days. The day that did not have hours missing was a Federal holiday with significant reduction in internet traffic—a factor that could have contributed to the absence of data. See Exhibit 2 for information regarding the hours captured and missed for our sampled days.

---

<sup>5</sup> We randomly selected the 5 days. See Exhibit 2 for the dates selected.

## Exhibit 2: Time Missing from [REDACTED] Tool



Source: OIG generated from data exports from [REDACTED] for the five days sampled (October 17 and 23, 2017; November 10, 2017; December 4 and 12, 2017.)

According to OIS, during initial implementation and rollout of [REDACTED], the [REDACTED] transmission service would stop without explanation. As a result, the Department implemented an alert that would identify when the [REDACTED] service stopped. According to OIS, since creating the alert, [REDACTED] has not experienced an outage. OIS also explained that [REDACTED] captured the hours not captured by [REDACTED]. Though [REDACTED] captured the information, the Department primarily utilizes [REDACTED] for reviewing and cataloging information. As a result, potential vulnerabilities may have gone undetected.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control AU-6 states, “The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.”

Failure to capture complete activity to a centralized location decreases the ability of an organization to correlate audit records across different repositories for organizational-wide situational awareness. Additionally, it increases the risk of wasteful and abusive activity going undetected, uninvestigated, and unresolved.

OIS stated that since initiating the alerts it had not experienced any instances of [REDACTED] not receiving the data from [REDACTED]. OIS provided data from [REDACTED] for an additional three days during February 2018 (February 23, 2018, February 26, 2018, and February 28, 2018). There was no missing data in the additional three days that we reviewed. As a result, OIG will not make a recommendation regarding this issue. OIS should continue to monitor the alerts to ensure that the [REDACTED] transmission continues to operate effectively.

## Conclusions

Although the Department had tools in place for monitoring, capturing, and reviewing internet usage and activities across the USCP network, we identified areas for improvement. Improving controls should not only ensure that the Department proactively identifies, categorizes, and reviews information but also ensure that the Department prevents the waste and abuse of internet resources.

**Recommendation 1:** We recommend that the United States Capitol Police, Office of Information Systems, consider tuning their [REDACTED] endpoint to deny [REDACTED] and allow [REDACTED] addresses, on an as-needed basis.

## Identifying and Responding to Waste and Abuse

Directive [REDACTED] states that the Department permits *de minimis* use of resources for personal use when “such uses are performed without measurable interference to the performance of the official duties.” However, the Directive does not define what the Department considers a measurable interference to an employee or contractor performance. The definition does not include internet activities deemed counterproductive or negatively affecting an employee’s productivity.

The Department also did not actively monitor USCP employee and contractor internet activity for waste or abuse. Because it primarily monitored internet traffic for malicious activity, OIS did not fully incorporate methods for monitoring internet activity for waste or abuse. OIS officials stated that supervisors could seek the assistance of OIS in determining whether employee internet usage constituted waste or abuse. OIG questions how OIS could measure waste and abuse in the absence of written guidance that clearly defines waste and abuse.

Additionally, URLs identified in [REDACTED] did not include the specific URL individuals accessed. The identified URLs were shortened names to specific websites associated with each URL. For example, [REDACTED] listed the URL visited as “youtube.com.” Because the reference was so broad, we could not determine whether such internet activity constituted a legitimate business use or waste and/or abuse. According to OIS officials, including detailed URLs in [REDACTED] would increase the cost beyond a reasonable amount.

## Conclusions

The Department did not fully define the term “measurable interference” in policies and procedures. Lack of a clear and concise definition increases the risk that overuse and/or abuse of the internet may go undetected, uninvestigated, or both. Additionally, without actual URLs visited listed in [REDACTED], the Department could not proactively identify waste and abuse.

**Recommendation 2:** We recommend that the United States Capitol Police define the term “measurable interference” and consider ways to implement alerts in Office of Information System’s tools to help identify waste and abuse.

**Recommendation 3:** We recommend that the United States Capitol Police, Office of Information Systems, conduct a cost benefit analysis to determine whether the benefit of incorporating Universal Resource Locator strings in [REDACTED] outweighs the additional cost.

# APPENDICES

## *List of Recommendations*

---

**Recommendation 1:** We recommend that the United States Capitol Police, Office of Information Systems, consider tuning their [REDACTED] endpoint to deny [REDACTED] [REDACTED] and allow [REDACTED] addresses, on an as-needed basis.

**Recommendation 2:** We recommend that the United States Capitol Police define the term “measurable interference” and consider ways to implement alerts in Office of Information System’s tools to help identify waste and abuse.

**Recommendation 3:** We recommend that the United States Capitol Police, Office of Information Systems, conduct a cost benefit analysis to determine whether the benefit of incorporating Universal Resource Locator strings in [REDACTED] outweighs the additional cost.

## DEPARTMENT COMMENTS

POLICE 202 224 5806



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

March 20, 2018

COP 180354

### MEMORANDUM

**TO:** Ms. 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 Monitoring of Internet Usage for Waste and Abuse* (Report No. OIG-2018-09)

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 Internet Usage for Waste and Abuse* (Report No. OIG-2018-09).

The Department generally agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon our internet usage monitoring capabilities. 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,

A handwritten signature in black ink, appearing to read "Matt Verderosa".

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 202-593-3868 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](mailto: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.

