UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Analysis of the
United States Capitol Police
Wireless Network and Devices

Report Number OIG-2019-14

September 2019

~~*REPORT RESTRICTION LANGUAGE*~~

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

This page intentionally left blank

TABLE OF CONTENTS

Abbreviations and Acronyms

Access Point	AP
Denial of Service	DoS
National Institute of Standards and Technology	NIST
Office of Information Systems	OIS
Office of Inspector General	OIG
Special Publication	SP
Standard Operating Procedure	SOP
United States Capitol Police	USCP or the Department
Wireless Local Area Network	WLAN

EXECUTIVE SUMMARY

In accordance with our *Annual Performance Plan Fiscal Year 2019*, the Office of Inspector General (OIG) conducted an analysis of the United States Capitol Police (USCP or the Department) wireless network and devices. OIG objectives were to determine if the Department (1) established adequate policies and procedures for the wireless network and devices, (2) established effective controls that would ensure the integrity of the wireless network and devices, and (3) complied with applicable laws, regulations, and guidance. Our scope included controls, processes, and operations from October 1, 2018, through June 30, 2019.

In Fiscal Year 2016, the Department's Office of Information Systems (OIS) began deploying a Wireless Local Area Network (WLAN). The WLAN was providing USCP wireless enabled devices with access to the USCP enterprise and internet connectivity. During our review, however, we identified gaps regarding documentation of security requirements and configurations as a result of the recent deployment of the WLAN and connected wireless enabled devices.

Specifically, USCP did not establish policies and procedures that would document control implementations clearly documented for configuration, connection requirements, or implementation guidance for wireless access and authorization of wireless connections. Further, while the Department uses [redacted] encryption on Apple iOS and Microsoft Surface wireless enabled devices, Department directives and standard operating procedures do not require implementation of [redacted]

USCP also did not establish effective controls that would ensure the integrity of the wireless network and devices. Specifically, USCP did not establish a process or methodology for assessing the WLAN security on a defined schedule. For example, we identified a wireless access point (AP) joined to the USCP enterprise with a potentially insecure configuration. OIS identified a setting on a wireless enabled device that appeared to be the cause of the identified AP. OIS officials took steps to remediate the device and stated that OIS plans to implement a configuration setting that will prevent similar devices from [redacted] in the future. Additionally, management consoles for USCP's wireless network controllers had [redacted] controls. For example, although OIS configured [redacted] requirements, the configuration was not enforced.

OIG made four recommendations as shown in Appendix A. On September 9, 2019, we provided a draft report to the Department for comment. We incorporated the Department's comments and attached their response in its entirety in Appendix B.

BACKGROUND

In Fiscal Year 2016, the Office of Information Systems (OIS) began the planning phase of the Wireless Local Area Network (WLAN) project. The United States Capitol Police (USCP or the Department) implemented the WLAN to augment a more mobile workforce and allow increased connectivity for newer technologies such as the Microsoft Surface Pros and Apple iPhones. USCP also designed implementation of the WLAN to decrease the amount of data consumption on mobile devices. USCP's *Project Charter Wireless Local Area Network*, dated April 10, 2017 stated that the Department will provide guest wireless access for outside agency representatives, vendors, and other scenarios yet to be determined. At the time of our analysis, the Department had not configured guest WLAN access.

The WLAN project consisted of deploying [redacted] wireless controllers and access points (APs) at USCP facilities including the Fairchild Building, Vehicle Maintenance Building, USCP Headquarters, Offsite Delivery/K-9 facility, and the Government Publishing Office building. OIS uses the [redacted] application to manage security policies for devices accessing APs. [redacted] would provide for the authentication mechanism for clients connecting to APs. We focused testing and analysis at the Fairchild Building and USCP Headquarters.

OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with our *Annual Performance Plan Fiscal Year 2019*, the Office of Inspector General (OIG) conducted an analysis of the USCP wireless network and devices. OIG objectives were to determine if the Department (1) established adequate policies and procedures for the wireless network and devices, (2) established effective controls to ensure the integrity of the wireless network and devices, and (3) complied with applicable laws, regulations, and guidance. Our scope included controls, processes, and operations from October 1, 2018, through June 30, 2019.

To accomplish our objectives, we interviewed officials from OIS, and reviewed documentation to gain an understanding of the wireless network as well as policies, procedures, controls, and configurations for wireless devices.

To determine compliance, we reviewed the following guidance, consisting of USCP Directives, Standard Operating Procedures (SOPs), and industry standards:

- USCP Directive [redacted], dated January 24, 2018.
- USCP Directive [redacted], dated January 9, 2018.
- USCP Directive [redacted], dated November 29, 2017.

- USCP SOP [redacted], dated August 14, 2017.
- USCP SOP [redacted], dated August 2, 2017.
- USCP Directive [redacted], April 21, 2017.
- USCP SOP [redacted] *Releases*, dated April 10, 2017.
- USCP SOP [redacted], dated September 14, 2016.
- USCP SOP [redacted], dated September 14, 2016.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*, dated April 2013.
- USCP Directive [redacted], dated October 19, 2012.
- USCP Directive [redacted], dated October 19, 2012.
- NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, dated February 2012.

As a legislative branch agency, USCP is not required to comply with NIST guidance; however, we used NIST guidance as a best practice.

OIG conducted this analysis in Washington, D.C., from May through August 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. On September 9, 2019, we provided a draft copy of this report to Department officials for comment. See Appendix A for a complete list of OIG recommendations. OIG incorporated Department comments as applicable and attached their response to the report in its entirety as Appendix B.

RESULTS

Overall, USCP did not have policies and procedures related to implementation of the wireless network. In addition, the Department did not have controls in place that could identify, detect, and prevent any potential security risks to the wireless network.

Inadequate Policies and Procedures

USCP policies related to the wireless network were not adequate. For example, the Department did not have a policy clearly documenting specific control implementations for configuration, connection requirements, or implementation guidance for wireless access and authorization of wireless connections. Additionally, while USCP used [redacted] encryption on Apple iOS and Microsoft Surface wireless enabled devices, USCP did not have directives or SOPs requiring [redacted].

Incomplete Documentation of Wireless Network Control Implementation

USCP did not have a policy clearly documenting specific control implementations for configuration, connection requirements, or implementation guidance for wireless access and authorization of wireless connections. Control AC-18 of NIST SP 800-53, Revision 4 states that policies and procedures should include establishment of usage restrictions, configuration and connection requirements, implementation guidance for wireless access, and authorization of wireless access to the information system prior to allowing such connections and encryption.

USCP documented the [redacted], dated August 22, 2017. Step twelve of the [redacted] for communications includes communication with leadership, the user community, and documenting official directives and SOPs. At the time of assessment, however, USCP had not reached that phase of the [redacted].

Without clear documentation of the requirements for a wireless network configuration, implementation guidance, or authorization of wireless connections, an increased risk existed for compromise by allowing non-authorized devices access to internal USCP resources.

Incomplete Documentation of Wireless Enabled Device Encryption Requirements

Although USCP was using [redacted] encryption on Apple iOS and Microsoft Surface wireless enabled devices, USCP did not have directives or SOPs requiring that [redacted]. Specifically, USCP Directive [redacted] defines encryption as, "The process of encoding data in such a way that unauthorized users cannot read it." However, the directive does not [redacted] Control AC-19 of NIST SP 800-53, Revision 4 states that organizations should employ full-device encryption or container encryption to protect the confidentiality and integrity of information on organization specified mobile devices.

Without [redacted] users may have misunderstood security requirements and used insecure wireless enabled devices for USCP business, potentially compromising USCP data confidentiality.

Conclusions

The Department lacked documented specific control implementations for the wireless network and requirements for wireless enabled encryption. Thus, OIG makes the following recommendations.

> **Recommendation 1: We recommend that the United States Capitol Police update its policies and procedures to document the wireless network control implementation, configuration, and authentication.**
>
> **Recommendation 2: We recommend that the United States Capitol Police update Directive [redacted] dated November 29, 2017, to include a [redacted] on wireless enabled devices.**

Lack of Internal Controls Related to the Wireless Network Implementation

The Department lacked internal controls related to implementation of the wireless network. For example, USCP did not establish a process or methodology for assessing the WLAN security on a set schedule. Although USCP documented a wireless security baseline checklist for the implementation of the [redacted] WLAN, as of June 24, 2019, the Department had not [redacted] policy, which required [redacted] for the wireless network controllers.

Gaps in Wireless Network Monitoring

USCP did not establish a process or methodology for assessing the WLAN security on a set schedule. A wireless AP in the Fairchild Building did not appear as part of the [redacted] wireless network. That AP also had a [redacted] enabled, which may have allowed cracking of the passphrase[1]. The device was assigned an internet protocol address on the USCP network. We communicated the information regarding the AP to OIS for investigation. OIS officials stated that they identified a setting on the device, which caused it to appear as an AP. OIS took steps to remediate the device and plans to implement a configuration setting that will prevent devices from [redacted] in the future.

NIST SP 800-153 states that organizations with WLANs should implement continuous monitoring solutions for their WLANs that provide detection capabilities including:

- Unauthorized WLAN devices, including rogue APs and unauthorized client devices.

[1] A passphrase used as a method of authentication to a wireless AP.

- WLAN devices misconfigured or using weak WLAN protocols and protocol implementations.

- Unusual WLAN usage patterns, such as extremely high numbers of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLAN in a short period of time.

- Use of active WLAN scanners that generate WLAN traffic. The use of passive sensors cannot be detected through monitoring controls.

- Denial of Service (DoS) attacks and conditions. DoS attacks are detected by counting events during periods of time and alerting when threshold values are exceeded. For example, a large number of events involving the termination of WLAN sessions can indicate a DoS attack.

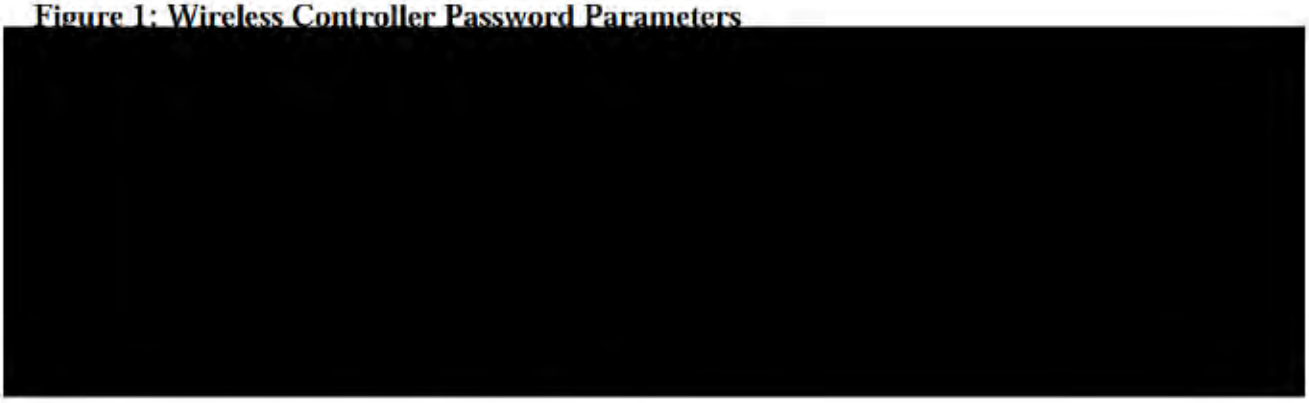
- Impersonation and man-in-the-middle attacks. For example, some Wireless Intrusion Detection and Prevention System sensors can detect when a device is attempting to spoof the identity of another device.

With the recent implementation of the USCP WLAN, OIS had not begun the continuous monitoring phase of the implementation. Without assessing the wireless network security from the aspect of an attacker, misconfigurations may go unnoticed and provide an avenue of compromise. In addition, [redacted] to the USCP network may allow an attacker access into the USCP enterprise.

Weak Wireless Network Controllers and Access Point Authentication

USCP documented a wireless security baseline checklist for implementation of the [redacted] WLAN. However, as of June 24, 2019, the Department had not enforced the [redacted], which required a [redacted] for the wireless network controllers. In addition, the [redacted] was set to "No." As a result, the [redacted] for the wireless controller was not enabled. See Figure 1 below for a screenshot of the wireless controller password parameter configuration.

Figure 1: Wireless Controller Password Parameters



The Department also did not configure the [redacted] may have allowed [redacted] wireless controllers.

Control IA-2 of NIST SP 800-53, Revision 4 indicates that moderate risk systems implement multifactor and replay resistant authentication for network and local access to privileged accounts. In addition, Control IA-5 of NIST SP 800-53, Revision 4 regarding authenticator management includes guidelines for enforcing minimum password complexity such as case sensitivity, number of characters, mix of upper and lower case letters, numbers and special characters.

USCP plans to implement centralized [redacted] through additional access control services when the guest wireless phase of the wireless network project is completed.

Without [redacted] implemented on wireless controllers and APs, a potential existed for [redacted] on the devices, which could have allowed an attacker to modify the device configuration.

Conclusions

USCP did not establish a process or methodology for assessing the WLAN security on a set schedule. Although USCP documented a wireless security baseline checklist for the implementation of the [redacted] WLAN, as of June 24, 2019, the Department had not [redacted] which required a [redacted] for the wireless network controllers. Thus, OIG makes the following recommendations.

> **<u>Recommendation 3</u>: We recommend that the United States Capitol Police document and implement a process for monitoring and assessing the wireless infrastructure for threats and risks on a periodic basis.**

Recommendation 4: We recommend that the United States Capitol Police implement [redacted] requirements for wireless network controllers and access points.

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police update its policies and procedures to document the wireless network control implementation, configuration, and authentication.

Recommendation 2: We recommend that the United States Capitol Police update Directive [redacted], dated November 29, 2017, to include a [redacted] on wireless enabled devices.

Recommendation 3: We recommend that the United States Capitol Police document and implement a process for monitoring and assessing the wireless infrastructure for threats and risks on a periodic basis.

Recommendation 4: We recommend that the United States Capitol Police implement [redacted] requirements for wireless network controllers and access points.

DEPARTMENT COMMENTS

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

September 20, 2019

COP 190585

MEMORANDUM

TO: Michael A. Bolton
Inspector General

FROM: Steven A. Sund
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Analysis of the United States Capitol Police Wireless Network and Devices* (Report No. OIG-2019-14)

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 Wireless Network and Devices* (Report No. OIG-2019-14).

The Department generally agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon the policies and procedures in place for the Wireless Network and Devices. The Department will assign Action Plans to appropriate personnel regarding each recommendation in effect in order 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,

Steven A. Sund
Chief of Police

cc: Chad B. Thomas, Acting 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

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