UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Performance Audit of the United States Capitol Police Mobile Device Program

Report Number OIG-2016-10

August 2016

~~REPORT RESTRICTION LANGUAGE~~

~~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

Abbreviations and Acronyms

Blackberry Enterprise Server	BES
Fiscal Year	FY
Government Accountability Office	GAO
Office of Information Systems	OIS
Office of Inspector General	OIG
Office of Professional Responsibility	OPR
National Institute of Standards and Technology	NIST
Property and Asset Management Division	PAMD
Personally Identifiable Information	PII
Special Publication	SP
Standard Operating Procedure	SOP
System Security Plan	SSP
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) administers the Department's mobile device program. Although the mobile device program consisted primarily of Blackberry devices, the Department also had several Android and Apple devices and a limited number of flip phones from various manufacturers.

In accordance with our annual plan, the Office of Inspector General (OIG) conducted a performance audit of the security of the Department's mobile device program. The objectives of this audit were to determine if USCP (1) established adequate internal controls and processes for ensuring security over Department-issued mobile devices, and (2) complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. The scope of the audit included controls, processes, and operations during Fiscal Year (FY) 2015 through January 2016. For the purposes of this audit, we considered cell phones and tablets as mobile devices. We excluded all other devices from the scope of this audit.

The Department did not have adequate controls that would ensure security over the mobile device program. The Government Accountability Office *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014) define internal controls as a process affected by an entity's oversight body, management, and other personnel in providing reasonable assurance that the entity achieves its objectives.

Although USCP established operating controls for mobile devices, some areas needed improvement. Those areas are as follows:

1. Developing and updating organizational wireless security policies and procedures addressing patching, use of Bluetooth technology, and vulnerability scanning for virus or malware on mobile devices.

2. Strengthening security over mobile devices, for example, sanitizing lost and stolen devices, whitelisting or blacklisting applications without an operational need. Those security procedures could prevent employees from installing third-party applications.

3. Developing and implementing a mechanism that could identify use of phone and data lines, which resulted in the Department paying for 59 phone lines that employees did not use during April 2016. Disconnecting unused lines could have resulted in about $3,000 in funds put to better use for the month of April 2016[1], or $36,000 annually.

[1] We tested for no, limited, and excessive usage as well as our testing for phone cramming, international, and roaming charges—we reviewed the entire usage report and detailed billing records for the month of April 2016.

4. Updating the official mobile device inventory records when employees separate from the Department.

Without written policies and procedures, users increase the risk of attackers hacking mobile devices and intercepting transmissions related to law enforcement sensitive information. Operating with controls that are out of date can result in OIS risking that its System Security Plan no longer meets the minimum-security requirements for mobile device management, which may potentially result in the breach of law enforcement sensitive data on mobile devices.

The Department did not always comply with policies and procedures. For example, OIS did not fully comply with baseline requirements for mobile device configurations documented in USCP Directive [redacted], dated October 19, 2012. In addition, USCP employees with access to Personally Identifiable Information (PII) on mobile devices did not sign annual compliance forms as USCP Directive [redacted] dated May 28, 2012, requires.

OIS has faced a turnover in key personnel and a shortage in budget, staffing, and training, which may have contributed to some of these control weaknesses and noncompliance issues. In January 2016, the Department hired a Director for OIS and OIG is hopeful this will assist in resolving these issues.

To develop more efficient and effective controls over the Department's mobile device program, ensuring security and support for business processes as well as the mission of USCP, we recommend that OIS establish detailed written internal controls and processes. The Department should also ensure compliance with current policies and procedures. See Appendix A for a complete list of OIG recommendations.

On July 28, 2016, OIG conducted an exit conference and on July 22, 2016 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 Department's mobile device program. As of April 21, 2016, the Department had 2,543 mobile devices identified in [redacted].[2] USCP's mobile device program consisted primarily of Blackberry devices. The Department also used Android and Apple devices as well as several flip phones from various manufacturers. OIS maintains three servers—the Blackberry Enterprise Server (BES) 5, BES 12, and the Good for Enterprise Server that manages USCP mobile devices. BES 5 manages older Blackberry devices and the BES 12 server manages newer Blackberry devices as well as Apple and Android devices. The Good for Enterprise Server also manages some Android and Apple devices. OIS officials stated that the Department is phasing out the Good for Enterprise Server.

[2] [redacted] is the official USCP system of record for all USCP personal property.

The Property and Asset Management Division (PAMD) is responsible for receiving and bar-coding devices when they arrive at USCP. PAMD also is responsible for recording inventory in the [redacted] system.

USCP obtains cellular service for their mobile devices from Verizon Wireless. The Department charges are through activation of new lines, which include unlimited data and minutes. The average cost for each line during April 2016 was $53.60.

OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with our annual plan, the Office of Inspector General (OIG) conducted a performance audit of the Department's mobile devices to determine if the Department (1) established adequate internal controls and processes for ensuring the security over issued mobile devices, 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 (FY) 2015 through January 2016. For the purposes of this audit, we considered cell phones and tablets as mobile devices. We excluded all other devices from the scope of this audit. In certain instances, such as our testing of mobile device usage during April 2016, we reviewed documentation after January 2016 because it was the most recently available information at the time of our testing.

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

- Number and type of Department-issued mobile devices
- Controls related to the mobile device program
- Vulnerability scanning and penetration testing OIS performed related to mobile devices
- Encryption of data on mobile devices
- Details of mobile device cellular plans
- Cellular usage on mobile devices
- Remote wiping of mobile devices

To determine compliance, we reviewed the following guidance:

- USCP [redacted], dated February 25, 2009

- USCP Standard Operating Procedure (SOP) [redacted] dated January 20, 2012
- USCP SOP [redacted], dated October 9, 2012
- USCP Directive [redacted], dated October 19, 2012
- USCP Directive [redacted], dated October 19, 2012
- USCP SOP [redacted], dated March 15, 2013
- USCP Directive [redacted] dated August 4, 2015

We also used Government Accountability Office (GAO) and 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 represent appropriate guidance and industry best practices for USCP.

We tested a random[3] sample of 32 of 1,120 phone lines as of April 2016 to determine if individuals with access to Personally Identifiable Information (PII) signed an annual PII-compliance agreement. In other testing—such as our test for no, limited, and excessive usage as well as our testing for phone cramming, international, and roaming charges—we reviewed the entire usage report and detailed billing records for the month of April 2016.

OIG conducted this performance audit in Washington, D.C., from February 2016 through July 2016, 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. On July 22, 2016, we provided a draft copy of this report to Department officials for comment. On July 28, 2016, we conducted an exit conference. We incorporated Department comments as applicable and attached its response to the report in its entirety as Appendix B.

[3] To generate our sample, OIG utilized the random number generator in Excel.

RESULTS

Overall, USCP did not have adequate internal controls and processes for ensuring the security of mobile devices as well as efficient and effective operations. The Department also did not always comply with best practices or policies and procedures related to mobile devices.

Inadequate Controls

The Department did not have adequate controls that would ensure security over the mobile device program. The GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014) define internal controls as a process affected by an entity's oversight body, management, and other personnel and providing reasonable assurance that the entity will achieve its objectives. GAO classifies objectives and related risks into one or more of the following categories:

- Operations – Effectiveness and efficiency of operations
- Reporting – Reliability of reporting
- Compliance – Compliance with applicable laws and regulations

Although USCP established some operating controls for mobile devices, some areas need additional improvement.

1. Developing and updating written policies and procedures
2. Improving security over mobile devices
3. Ensuring separated employees return devices and updating the inventory records at that time
4. Implementing proper segregation of duties by ensuring that system owners of System Security Plans (SSP) are not also signing Authorizations to Operate for the same systems.

The Department did not have a mechanism for identifying phone lines that had no, limited, or excessive use. As a result, the Department paid for 59 phone lines that employees did not use during April 2016. Disconnecting lines that were unused could have resulted in about $3,000 of funds put to better use for the month of April 2016, or $36,000 annually. Without adequate internal controls, USCP mobile devices may contain vulnerabilities and weaknesses that attackers could exploit.

Lack of or Outdated Policies and Procedures

OIS lacked sound security policies and procedures related to mobile device patching, Bluetooth applications, and vulnerability scanning. OIS also utilized outdated mobile device policies and procedures.

NIST Special Publication (SP) 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, dated June 2014, states, "At a minimum, all components should be updated with the latest available patches and configured following sound security practices." However, USCP lacked policies and procedures related to its internal process for patching mobile device operating systems. According to OIS officials, Blackberry devices receive manual updates only when users bring the device in for service. Android and Apple device users could have installed patches at their discretion.

OIS also did not have an operating policy for the security of Bluetooth-enabled devices. NIST SP 800-121, Revision 1, *Guide to Bluetooth Security*, dated June 2012 states:

> Organizations using Bluetooth technology should establish and document security policies that address the use of Bluetooth-enabled devices and users' responsibilities. Organizations should include awareness-based education to support staff understanding and knowledge of Bluetooth. Policy documents should include a list of approved uses for Bluetooth and the type of information that may be transferred over Bluetooth networks. The security policy should also specify a proper password usage scheme. When feasible, a centralized security policy management approach should be used in coordination with an endpoint security product installed on the Bluetooth devices to ensure that the policy is locally and universally enforced.

OIS also did not define, develop, or document a vulnerability scanning policy covering virus and malware scanning for mobile devices. OIS further did not scan mobile devices for viruses and malware. However, best practices guidance such as NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, states,

> The organization:
>
> a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported.

NIST SP 800-124, Revision 1, states:

> Operational processes that are particularly helpful for maintaining mobile device security, and thus should be performed regularly, include the following:
>
> Organizations should also periodically perform assessments to confirm that the organization's mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing. More information on technical assessments is available from NIST SP 800-115, Technical Guide to Information Security Testing and Assessment [SP 800-115].

Likewise, the controls for security documentation of mobile devices contained were out of date. OIS referenced controls in its SSP that were about 10 years old. For example, the controls for BES 12 contained references to NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, dated July 2002. However, NIST revised SP 800-30 in September 2012. Our testing revealed:

- Of the 16 governing controls reviewed in the SSP for BES 12, 8 were out of date.
- Of the11 governing controls reviewed for the BES 12 Security Assessment Report, 8 were out of date.
- Of the 15 governing controls reviewed for the BES 12 Risk Assessment Report, 7 were out of date.

See Appendix C for list of outdated controls.

Without written procedures covering wireless security policy that address patching, use of Bluetooth technology, and vulnerability scanning for malware on mobile devices, the Department remains vulnerable and susceptible to threats that could result in attacks. Operating with outdated controls also has OIS running the risk that its SSP no longer meets the minimum-security requirements for mobile device management, which may potentially result in the breach of law enforcement sensitive data on mobile devices.

Inadequate Security over Mobile Devices

OIS did not have adequate security addressing sanitizing and whitelisting related to its mobile device program. NIST SP 800-53, Revision 4, states:

> The organization:
>
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
> 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
>
> b. Reviews and updates the current:
>
> 1. Media protection policy [Assignment: organization-defined frequency]; and
> 2. Media protection procedures [Assignment: organization-defined frequency].

NIST SP 800-53, Revision 4 further states:

> The organization:
>
> a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

OIS stated that if a device is lost or stolen that it will send out a command to sanitize the mobile device, but neither OIS nor USCP's [redacted], dated February 25, 2009, documents details about remotely wiping lost/stolen devices. As a result, OIS runs the risk of not following consistent procedures for remotely wiping lost or stolen mobile devices, which may result in missed critical steps for sanitizing mobile devices.

Although it created a list of applications that were whitelisted[4] for Blackberry devices, OIS did not create a whitelist for Android and Apple devices. OIS also did not include preinstalled Blackberry applications on the whitelist. For example, Blackberry devices contained preinstalled applications such as Facebook, Twitter, and YouTube, and the need for such applications was not clear. NIST SP 800-124, Revision 1, states, "Restrict which applications may be installed through whitelisting (preferable) or blacklisting." NIST SP 800-53, Revision 4, states:

> The organization:
>
> a. Identifies [Assignment: organization-defined software programs not authorized to execute on the information system];
> b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
> c. Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].

According to OIS officials, the BES 12 used to manage Android and Apple devices did not have the ability to create a whitelist for Android and Apple devices. Without implementation of a whitelisting solution that covers all mobile device platforms, OIS runs the risk of enabling users operating Apple and Android devices the ability to install untrusted third-party applications. Additionally, OIS would not be able to verify that mobile device applications receive only the necessary security permissions, which may result in the breach of USCP data.

Lack of Mechanism to Identify No, Limited, or Excessive Usage of Mobile Devices

The GAO *Standards for Internal Control in the Federal Government* states, "Management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose." In addition, USCP Directive [redacted], dated August 4, 2015, states

> It is the policy of the USCP that official USCP resources may only be used in connection with official business. However, in recognition of the infrequent need for authorized users of official USCP resources or equipment to take care of occasional personal matters during normal business hours, *de minimis* use of official USCP resources and equipment, (i.e., computers, laptops, BlackBerry devices, Internet services, cellular phones, copiers, faxes, and other such similar devices) is permitted subject to the limitations in this and other directives.

[4] Application whitelisting is a computer administration practice for preventing unauthorized programs from running.

OIS did not have a mechanism for identifying phone lines with no or limited use. During April 2016, USCP paid about $3,000 for 59 phone lines that were not used during that month. According to OIS officials, OIS activates and deactivates lines on a regular basis. Based on the April 2016 usage rate, however, if the Department deactivated the unused phone lines in a timelier manner, the Department would save about $36,000 annually.

We also identified several phone lines that had limited use during April 2016. OIS stated that the Department keeps many emergency-use-only phone lines. Yet, OIS could not provide a list of emergency-use-only lines and, as such, OIS did not have a process for identifying phone lines without an operational need. OIS stated that it plans to implement monitoring procedures for identifying lines with no or limited use to mitigate the costs of unused lines.

OIS did not have a process that would identify phone lines with excessive use. We reviewed a detailed usage report for April 2016 and identified several lines with excessive voice and data use. For example, we noted one phone line, issued to a Private First Class in the Patrol Division that used 5,697 minutes during April 2016. A review of the detailed phone records for the line showed many calls to several phone numbers in Delaware. In another example, an OIS contractor used more than 90 gigabytes of data and a Sergeant in the Investigations Division used more than 86 gigabytes of data on Department-issued phones. According to OIS, exception reports can be prepared for USCP management to verify and validate operational needs.

Of the Department's 1,120 phone lines, 6 lines used more than approximately 3,000 minutes of voice usage and 5 lines with more than 20 gigabytes of data usage during April 2016. According to an article published by *The Motley Fool* on January 24, 2015, the average wireless customer consumes 1.8 gigabytes of data per month. OIG did not perform additional procedures to determine the nature of the usage, but the Department did not perform any monitoring to determine if there was an operation need for the usage. Because most USCP phone plans have unlimited minutes and data, the excessive usage did not cost extra. However, the cost to USCP may be foregone utility of personnel. OIG Audits referred the excessive use matter to OIG Investigations and the Office of Professional Responsibility (OPR).

Inadequate Inventory of Mobile Devices

PAMD and OIS did not maintain an accurate inventory of mobile devices. NIST SP 800-124, Revision 1, states:

> Operational processes that are particularly helpful for maintaining mobile device security, and thus should be performed regularly, include the following: Keeping an active inventory of each mobile device, its user(s), and its applications.

[redacted] provides an inventory of each user of mobile devices. We compared a listing of separated employees to the [redacted] inventory and found six former employees with mobile devices recorded in [redacted] Of the six former employees, one had two devices recorded in [redacted] OIS stated that some of the devices could be in OPR. OPR, however, did not have the devices. Without sufficient monitoring of controls of device users who have separated from the

Department, USCP runs the risk of maintaining active mobile devices that could be in the possession of separated employees, which could also result in unauthorized access to law enforcement sensitive data. Subsequently, after we conducted our exit conference, OIS was able to physically account for 6 of the 7 mobile devices. OIS provided us additional information for the other device indicating that it was reported lost by the employee.

Inadequate Segregation of Duties

GAO *Standards for Internal Control in the Federal Government* state,

> Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibly for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event.

Yet, USCP did not appropriately segregate the duties for the SSP related to the BES 12 server. The same individual was the system owner on the SSP related to the BES 12 server and signed the Authorization to Operate. Without proper segregation, USCP is vulnerable to error, misuse, or fraud. In 2016, the Department hired a director for OIS, which should assist in segregating key duties and responsibilities.

Conclusions

The Department did not have adequate policies and procedures or controls in place for ensuring security and integrity of the Department's mobile device program. Weaknesses in controls could place its mobile device operations at an increased risk for vulnerabilities that may lead to a data breach. We, therefore, make the following recommendations.

Recommendation 1: We recommend that the United States Capitol Police Office of Information Systems develop and fully implement policies and procedures to update mobile devices with the latest available patches, Bluetooth technology in accordance with best practices, and scanning systems and applications. The Office of Information Systems should further update its security assessment policies and procedures for mobile devices to reflect the use of current operating controls ensuring the System Security Plan meets the minimum-security requirements for mobile device management.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems develop, document, and disseminate policies and procedures for media protection that includes destroying or sanitizing mobile devices using approved equipment, techniques, and procedures ensuring consistent procedures for remotely wiping lost or stolen mobile devices.

Recommendation 3: We recommend that the United States Capitol Police Office of Information Systems identify and fully implement a whitelisting solution that covers all mobile device platforms operated by employees and contractors by whitelisting and

vetting all third party applications (including pre-installed applications) before deployment of official mobile devices.

Recommendation 4: We recommend that the United States Capitol Police Office of Information Systems develop a mechanism that will identify lines with no or limited use and inquire with the Department on a monthly basis to determine if the Office of Information Systems should discontinue the service, which could result in annual cost savings of about $36,000. The Office of Information Systems also should monitor detailed phone usage reports, identify lines with excessive usage, and send a report to the applicable Bureau to inquire if the usage was commensurate with the phone holder's responsibilities. Such monitoring should also identify emergency-use-only lines.

Recommendation 5: We recommend that the United States Capitol Police Office of Information Systems create an efficient process for maintaining an accurate and up-to-date inventory of its mobile devices, including procedures for obtaining and deactivating mobile devices of separated employees, thereby reducing the risk of unauthorized access to Law Enforcement Sensitive Data.

Recommendation 6: We recommend that the United States Capitol Police implement proper segregation of duties by ensuring that system owners of System Security Plans are not also signing Authorizations to Operate for the same systems.

Noncompliance with Policies and Procedures

USCP did not always comply with its policies and procedures. For example, mobile device configuration baselines did not comply with USCP password policy. In addition, USCP employees with access to PII on mobile devices did not sign an annual compliance form as USCP Directive [redacted], dated May 28, 2012, requires. As a result, USCP runs the risk of employees and contractors neglecting the importance of compliance, which may result in an unauthorized disclosure of PII.

Noncompliance with Mobile Device Configuration Baseline

Mobile device configuration baselines did not fully comply with the requirements documented in the USCP Directive [redacted], dated October 19, 2012, which states the following:

> 2. Strong passwords are at least eight alphanumeric characters in length . . .
> 7. Passwords must be changed every 60 days.
> The system will remember up to 24 passwords, therefore, the same password cannot be reused.
> 8. Screensavers should activate when there is 15 minutes of inactivity.

In several instances, the mobile device configuration baseline did not follow the requirements in Directive [redacted]. See Tables 1-3 below for a comparison of the configuration settings and Directive [redacted]

Table 1 - Blackberry Enterprise Server 5 Configuration		
Configuration Setting	Current Setting	USCP Directive Requirement
Maximum security timeout	30 minutes	15 minutes
Minimum password length	8 characters	8 characters
Maximum password age	60 days	60 days
Minimum password history	3 previous passwords	24 previous passwords
Set password timeout	15 minutes	15 minutes

Source: OIG-generated comparison of current configuration settings to requirements in Directive [redacted]

Table 2 - Blackberry Enterprise Server 12 Configuration		
Configuration Setting	Current Setting	USCP Directive Requirement
Lock work space after inactivity	30 minutes	15 minutes
Minimum password length	8 characters	8 characters
Maximum password age	90 days	60 days
Number of previous passwords checked	4 previous passwords	24 previous passwords
Lock work space after inactivity	30 minutes	15 minutes

Source: OIG-generated comparison of current configuration settings to requirements in Directive [redacted]

Source: Photo of Blackberry Bold 9950 and Blackberry Classic obtained from us.blackberry.com

[redacted]

Table 3 – Good for Enterprise Server Configuration		
Apple Configuration		
Configuration Setting	Current Setting	USCP Directive Requirement
Lock work space after inactivity	30 minutes	15 minutes
Require passcode	1 character	8 characters
Maximum passcode age	No	60 days
Passcode history	No	24 previous passwords
Auto-lock	No	15 minutes
Alphanumeric	No	Digits, punctuations, letters, and at least 8 alphanumeric characters
Minimum number of complex characters	No	Recommends use of digit and punctuation characters but does not specify a minimum number of complex characters
Android Configuration		
Configuration Setting	Current Setting	USCP Directive Requirement
Lock work space after inactivity	30 minutes	15 minutes
Minimum length of passcode	8 characters	8 characters
Maximum passcode age	90 days	60 days
Passcode history	3 previous passwords	24 previous passwords
Auto-lock	No	15 minutes
Alphanumeric	Yes	Digits, punctuations, letters, and at least 8 alphanumeric characters
Complex	No	Recommends the use of digit and punctuation characters but does not specify a minimum number of complex characters

Source: OIG-generated comparison of current configuration settings to requirements in Directive [redacted]

Mobile devices that do not comply with configuration baselines have an increased risk of breaches occurring in the event that they are lost or stolen. Noncompliance probably occurred because of the significant turnover of OIS staff. As stated previously, the Department hired a director for OIS in FY 2016.

Noncompliance with Personally Identifiable Information

USCP employees with access to PII on mobile devices did not sign an annual compliance form as required by USCP Directive [redacted], which states:

> Department officials, employees and contractors, after receiving online training, will be required to sign an annual compliance form certifying that they have received, understand, and agree to comply with all policies and procedures covered in this Directive. Failure to sign the form or to otherwise comply with the policies and procedures may result in denial of access to Department information, the Department network, or other Information Technology (IT) resources, or more serious disciplinary action, where appropriate.

A random sample of 32 employees with access to PII on mobile devices did not sign an annual PII compliance form. The Department could not provide annual compliance forms for any of the employees selected in our sample. OIS did not explain the missing compliance forms. As a result, USCP runs the risk of employees and contractors neglecting the importance of compliance, which may result in an unauthorized disclosure of PII.

Conclusions

USCP mobile device configurations did not comply with Department policies and procedures. The Department also did not comply with USCP Directive [redacted], which requires that employees with access to PII sign and annual compliance form. We, therefore, make the following recommendations:

Recommendation 7: We recommend that the United States Capitol Police Office of Information Systems modify the configuration baseline settings for mobile devices to ensure that they comply with Directive [redacted] dated October 19, 2012.

Recommendation 8: We recommend that the United States Capitol Police adhere to the annual Personally Identifiable Information compliance requirement outlined in Directive [redacted] dated May 28, 2012, which requires that employees sign an annual compliance form.

[redacted]

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police Office of Information Systems develop and fully implement policies and procedures to update mobile devices with the latest available patches, Bluetooth technology in accordance with best practices, and scanning systems and applications. The Office of Information Systems should further update its security assessment policies and procedures for mobile devices to reflect the use of current operating controls ensuring the System Security Plan meets the minimum-security requirements for mobile device management.

Recommendation 2: We recommend that the United States Capitol Police Office of Information Systems develop, document, and disseminate policies and procedures for media protection that includes destroying or sanitizing mobile devices using approved equipment, techniques, and procedures ensuring consistent procedures for remotely wiping lost or stolen mobile devices.

Recommendation 3: We recommend that the United States Capitol Police Office of Information Systems identify and fully implement a whitelisting solution that covers all mobile device platforms operated by employees and contractors by whitelisting and vetting all third party applications (including pre-installed applications) before deployment of official mobile devices.

Recommendation 4: We recommend that the United States Capitol Police Office of Information Systems develop a mechanism that will identify lines with no or limited use and inquire with the Department on a monthly basis to determine if the Office of Information Systems should discontinue the service, which could result in annual cost savings of about $36,000. The Office of Information Systems also should monitor detailed phone usage reports, identify lines with excessive usage, and send a report to the applicable Bureau to inquire if the usage was commensurate with the phone holder's responsibilities. Such monitoring should also identify emergency-use-only lines.

Recommendation 5: We recommend that the United States Capitol Police Office of Information Systems create an efficient process for maintaining an accurate and up-to-date inventory of its mobile devices, including procedures for obtaining and deactivating mobile devices of separated employees, thereby reducing the risk of unauthorized access to Law Enforcement Sensitive Data.

Recommendation 6: We recommend that the United States Capitol Police implement proper segregation of duties by ensuring that system owners of System Security Plans are not also signing Authorizations to Operate for the same systems.

Recommendation 7: We recommend that the United States Capitol Police Office of Information Systems modify the configuration baseline settings for mobile devices to ensure that they comply with Directive [redacted] dated October 19, 2012.

Recommendation 8: We recommend that the United States Capitol Police adhere to the annual Personally Identifiable Information compliance requirement outlined in Directive [redacted] dated May 28, 2012, which requires that employees sign an annual compliance form.

DEPARTMENT COMMENTS

PHONE: 202-224-9806

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

July 29, 2016

COP 160177

MEMORANDUM

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

FROM: Matthew R. Verderosa
Chief of Police

SUBJECT: Response to Office of Inspector General (OIG) draft report *Performance Audit of the United States Capitol Police Mobile Device Program* (Report No. OIG-2016-10).

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 *Performance Audit of the United States Capitol Police Mobile Device Program* (Report No. OIG-2016-10).

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

Very respectfully,

Matthew R. Verderosa
Chief of Police

cc: Richard Braddock, Chief Administrative Officer
[redacted] USCP Audit Liaison

Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.

Outdated Controls

Blackberry Enterprise Server 12 System Security Plan		
Reference Used	**Current Reference**	**Updated Reference**
E-Government Act (Public Law 107-347), Title III, *Federal Information Security Management Act (FISMA)*, December 2002	Current	
Office of Management and Budget (OMB) Circular A-130 Appendix III, *Security of Federal Automated Information Resources*, November 2000	Current	
Federal Information Processing Standard (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004	Current	
FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006	Current	
FIPS PUB 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006	Outdated	FIPS 201-2 Aug. 2013
NIST SP 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model*, April 1998	Current	
NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006	Current	
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002	Outdated	SP 800-30 Rev. 1 Sep. 2012
NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002	Outdated	SP 800-34 Rev. 1 May 2010
NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004	Outdated	SP 800-37 Rev. 1 Feb 2010
NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002	Current	
NIST SP 800-50, Building an Information Technology Security Awareness and Training Program dated October 2003	Current	

Outdated Controls

Blackberry Enterprise Server 12 System Security Plan (Continued)		
Reference Used	**Current Reference**	**Updated Reference**
NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009	Outdated	SP 800-53 Rev. 4 Apr. 2013
NIST Draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, April 26, 2006	Outdated	SP 800-53 A Rev. 4 Dec. 2014
NIST SP 800-60 Version 2.0, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and Volume II, *Appendixes*, June 2004	Outdated	SP 800-60 Volume II Rev. 1 Aug. 2008
NIST SP 800-64 Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004	Outdated	SP 800-64 Rev. 2 Oct. 2008
Source: OIG generated from review of BES 12 System Security Plan.		

Blackberry Enterprise Server 12 Security Assessment Report		
Reference Used	**Current Reference**	**Updated Reference**
FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004	Current	
FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006	Current	
NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009	Outdated	SP 800-53, Rev. 4, Apr. 2013
NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, August 2009	Outdated	SP 800-53, A Rev. 4, Dec. 2014
NIST SP 800-18, Revision1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006	Current	
NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002	Outdated	SP 800-30 Rev. 1 Sep. 2012

Outdated Controls

Blackberry Enterprise Server 12 Security Assessment Report (Continued)		
Reference Used	**Current Reference**	**Updated Reference**
NIST SP 800-26, Revision1, *Security Self-Assessment Guide for Information Technology Systems*, November 2001	Outdated	Archived Feb. 2007. Superseded by FIPS 200, SP 800-53, and SP 800-53A.
NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004	Outdated	SP 800-37 Rev. 1 Feb. 2010
NISP SP 800-42, *Guideline on Network Security Testing*, October 2003	Outdated	Archived Sep. 2008. Superseded by SP 800-115
NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004	Outdated	SP 800-60 Volume II Rev. 1 Aug. 2008
NIST SP 800-63 *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, December 2011	Outdated	SP 800-63 Rev. 2 Aug. 2013
Source: OIG generated from review of BES 12 Security Assessment Report.		

Blackberry Enterprise Server 12 Risk Assessment Report		
Reference Used	**Current Reference**	**Updated Reference**
E-Government Act (Public Law 107-347), Title III, Federal *Information Security Management Act* (FISMA), December 2002	Current	
OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*, November 2000	Current	
Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004	Current	

Outdated Controls

Blackberry Enterprise Server 12 Risk Assessment Report (Continued)		
Reference Used	**Current Reference**	**Updated Reference**
FIPS PUB 200, *Minimum Security Controls[Requirements] for Federal [Information and Information] Systems*, March 2006	Current	
FIPS PUB 201-1, *Personal Identity Verification for Federal Employees and Contractors*, June [March] 2006	Outdated	FIPS 201-2 Aug. 2013
NIST SP 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model*, April 1998	Current	
NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006	Current	
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002	Outdated	SP 800-30 Rev. 1 Sep. 2012
NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002	Outdated	SP 800-34 Rev. 1 May 2010
NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004	Outdated	SP 800-37 Rev. 1 Feb. 2010
NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002	Current	
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003	Current	
NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, October [August] 2009	Outdated	SP 800-53 Rev 4 Apr. 2013
NIST SP 800-60 Version 2.0, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and Volume II, *Appendixes*, June 2004	Outdated	SP 800-60 Rev. 1 Aug. 2008
NIST SP 800-64 Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004	Outdated	SP 800-64 Rev. 2 Oct. 2008
Source: OIG-generated from review of BES 12 Risk Assessment Report.		

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 20510

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