UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Performance Audit of the
United States Capitol Police
Public Web Site and Web Applications

Report Number OIG-2016-05

March 2016

~~Report Restriction Language~~

~~Distribution of this Document is Restricted~~

~~This report contains sensitive law enforcement material and is the property of the Office of the Inspector General and is intended solely for the official use of the United States Capitol Police, the Capitol Police Board, or any agency or organization receiving the report directly from the Office of Inspector General. No Secondary distribution may be made, in whole or in part, outside the United States Capitol Police or Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports OIG prepares periodically as part of its oversight responsibility with respect to the United States Capitol Police (USCP) to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG and discussed the draft with those responsible for implementation. It is my hope that the recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to those contributing to the preparation of this report.

Fay F. Ropella

Fay F. Ropella, CPA, CFE
Inspector General

TABLE OF CONTENTS

[redacted]

Abbreviations and Acronyms

Certification and Accreditation	C&A
Chief Information Security Officer	CISO
Council of the Inspectors General on Integrity and Efficiency	CIGIE
Department of Homeland Security	DHS
Federal Information Security Management Act of 2002	FISMA
Federal Information Security Modernization Act of 2014	FISMA
Fiscal Year	FY
Government Publishing Office	GPO
Information Technology	IT
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
Office of Policy and Management Systems	OPOL
Peace Officer Background Investigation Tracking System	POBITS
Personally Identifiable Information	PII
Plan of Action and Milestones	POA&M
National Aeronautics and Space Administration	NASA
National Institute of Standards and Technology	NIST
Risk Management Framework	RMF
United States Capitol Police	USCP or the Department
Virtual Private Network	VPN

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) maintains its public Web site at uscapitolpolice.gov. The Government Publishing Office (GPO), who provides Web hosting services for several agencies, hosts the Department's site. In addition to the public Web site, the Department also maintains two other public Web applications—the Peace Officer Background Investigation Tracking System (POBITS) and a virtual private network (VPN) portal. POBITS is a Web-based application the Department uses for conducting background investigations during the hiring process. The VPN portal is a Web application that allows Department employees to remotely access the USCP network through a VPN.

In accordance with our annual plan, the Office of Inspector General (OIG) conducted a performance audit of the security of the USCP public Web site and the two public Web-based applications. The objectives of this audit were to determine if USCP (1) established adequate internal controls and processes for ensuring Web site application security and efficient and effective operations, and (2) complied with applicable laws, regulations, and guidance pertaining to management and operation of its publicly accessible Web applications. The scope included controls, processes, and operations during Fiscal Years (FYs) 2014 and 2015.

Overall, the Department did not establish adequate internal controls and processes for ensuring Web site application security and efficient and effective operations. For example, the Department did not have evidence of a Memorandum of Agreement or Memorandum of Understanding between GPO and USCP regarding GPO hosting of the Department Web site. Without such an agreement, USCP has no documented understanding of expectations and/or procedures for security controls of its public Web site. As such, the Department cannot enforce accountability as required by Principle 5, *Enforcement of Accountability*, as required by the *Standards for Internal Control in the Federal Government*[1], dated September 2014.

In a previous audit—*Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program*, Audit Report Number OIG-2015-10, dated September 2015—OIG recommended that the Department adopt the National Institute of Standards and Technology's (NIST) risk management framework (RMF) for its security controls. An RMF is the unified information security framework for the entire Federal Government that is replacing the legacy Certification and Accreditation (C&A) processes within its departments and agencies. With an RMF, the Department would have prevented many of the internal control weaknesses identified during the audit. As of February 2016, the Office of Information Systems (OIS) continues with its efforts to implement the NIST RMF. According to an OIS official, adopting an RMF is a time-consuming process.

The Department also did not have adequate written policies and procedures governing the use of Web applications. USCP Directive [redacted], dated February 3,

[1] United States Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, dated September 2014.

2014, discusses public facing Web sites and local Intranets. Specifically, OIS did not have any policies or procedures addressing Web applications such as POBITS or the VPN portal. The Department also did not comply with USCP Directive [redacted] dated October 19, 2012, with respect to system level passwords for the VPN portal.

Because USCP is a legislative-branch entity, it is exempt from many of the laws and regulations that apply to executive-branch agencies; however, these laws and regulations represent appropriate guidance and industry best practices for USCP. On December 17, 2002, the President signed into law the E-Government Act, including Title III, the Federal Information Security Management Act (FISMA) (Title III, Pub. L. No. 107-347). On December 8, 2014, the President signed into law the Federal Information Security Modernization Act (FISMA), which replaced the 2002 FISMA legislation. FISMA requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of the management, operational, and technical controls over Information Technology (IT) that support operations and assets.

Yet, the privacy policy for the USCP Web site did not comply with the FISMA dated 2002. FISMA requires that Web sites of Federal agencies include a privacy policy for information the site collects, with whom information is shared, and the intended use of the information. As of January 27, 2016, the privacy policy on USCP's Web site makes multiple references to the Department of Homeland Security (DHS) site rather than the USCP Web site. This probably occurred because USCP copied the privacy policy from the DHS Web site and did not change all references of DHS to USCP. As of February 26, 2016, the Department had corrected the DHS references.

To develop more efficient and effective controls over the USCP Web site and Web applications, we repeat the previous OIG recommendation[2] that the Department identify an appropriate RMF and develop policies and procedures for implementing the chosen framework. The Department should also develop policies and procedures related to its public Web applications. See Appendix A for a complete list of OIG recommendations.

On February 10, 2016, OIG conducted an exit conference and 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

In accordance with our annual plan, the Office of Inspector General (OIG) conducted a performance audit of the security of the United States Capitol Police (USCP or the Department) public Web site and Web applications.

[2] *Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program*, OIG-2015-10, dated September 2015, Recommendation 1.

The Department maintains its public Web site at uscapitolpolice.gov. In addition, the Department maintains two public facing Web applications—the Peace Officer Background Investigation Tracking System (POBITS) and a Virtual Private Network (VPN) portal. The POBITS is a Web application the Department uses for collecting information from candidates who apply for positions as sworn police officers in order to conduct background investigations. The VPN portal is another Web application the Department uses that allows employees to access the USCP network through a VPN connection.

The Government Publishing Office (GPO) hosts the Department's public Web site, uscapitolpolice.gov. GPO officials stated that GPO has been hosting the USCP Web site for at least 12 years, although no evidence of an initial agreement between GPO and USCP exists.

According to USCP Directive [redacted], dated February 3, 2014, each bureau or office has a Web Content Contributor. Web Content Contributors are responsible for making sure that the Web site content for their bureau or office is correct. If changes to the Web site are required, the Web Content Contributors notify the Web Content Manager in the Office of Policy and Management Systems (OPOL). The Content Manager then works with GPO to make changes to the USCP Web site. The Public Information Officer also has authority to work with GPO to post Web site content. During October 2015, the public Web site received 549,276 page views.

POBITS is a public Web-based application departments can buy and then host for collecting background investigation information from candidates applying to the Department for employment. According to the POBITS Web site, "POBITS gives your department a comprehensive standardized method for conducting investigations and producing consistent review packages for evaluating your candidate's suitability for a position in law enforcement or public safety." Candidates applying to USCP input information into POBITS. Although POBITS contains Personally Identifiable Information (PII), Department officials stated that USCP encrypts PII collected through POBITS while in transit over the Internet. The application does not, however, [redacted]. The Office of Information Systems (OIS) is responsible for hosting POBITS. In addition, the Office of Human Resources (OHR) has a role in creating user accounts for candidates in POBITS.

The VPN portal is another public Web-based application, and allows Department employees to connect to the USCP network from any computer connected to the Internet. Logging into the VPN portal requires two-step authentication using the employee's network username and password as well as a one-time password token. OIS is responsible for hosting and all controls related to the VPN portal.

USCP also maintains PoliceNet, which is a local Intranet site. PoliceNet is used for sharing information within the Department. We did not include this site as part of our audit because the scope of our audit included only public facing sites.

Because USCP is a legislative-branch entity, it is exempt from many of the laws and regulations that apply to executive-branch agencies; however, these laws and regulations represent appropriate

guidance and industry best practices for USCP. On December 17, 2002, the President signed into law the E-Government Act, including Title III, the Federal Information Security Management Act (FISMA) (Title III, Pub. L. No. 107-347). On December 8, 2014, the President signed into law the Federal Information Security Modernization Act (FISMA), which replaced the 2002 FISMA legislation. FISMA requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of the management, operational, and technical controls over Information Technology (IT) that support operations and assets.

OBJECTIVES, SCOPE, AND METHODOLOGY

OIG conducted this performance audit to determine if the Department (1) established adequate internal controls and processes for ensuring Web site application security and efficient and effective operations, and (2) complied with applicable laws, regulations, and guidance pertaining to management and operation of its publicly accessible Web applications. Our scope for this audit included controls, policies, and procedures during Fiscal Years (FYs) 2014 and 2015.

To accomplish our objectives, we communicated with the Chief Information Security Officer and other OIS personnel and reviewed documentation to gain an understanding of the following areas:

- Number and type of Web applications
- Controls related to uscapitolpolice.gov, POBITS, and the VPN portal
- Vulnerability scanning and penetration testing performed by OIS related to POBITS and VPN portal
- GPO's role in the hosting of uscapitolpolice.gov

To determine compliance, we reviewed the following guidance:

- USCP Directive [redacted], dated February 3, 2014.

We obtained a sample audit work plan from the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The National Aeronautics and Space Administration (NASA) developed the work plan provided to OIG. Because of the large volume of information it shares with the public, NASA has many public Web sites and Web applications. USCP has a much smaller Web presence than NASA. We adapted the NASA work plan to reflect the Department's smaller Web presence.

During our audit, we queried OIS officials, who informed OIG that the Department has one public Web site (uscapitolpolice.gov) and two public Web-based applications (POBITS and the VPN

portal). Because of the small number of Web sites and applications, we selected the Web site and both of the public Web-based applications for our detailed testing.

To ensure the adequacy of internal controls over the Web site, we queried OIS regarding the controls. OIS stated that OPOL is responsible for notifying GPO of any edits needed to the Web site and that GPO is responsible for all other controls surrounding the Web site. We discussed the agreement between USCP and GPO with that agency and requested the agreement between USCP and GPO to verify the existence of these controls.

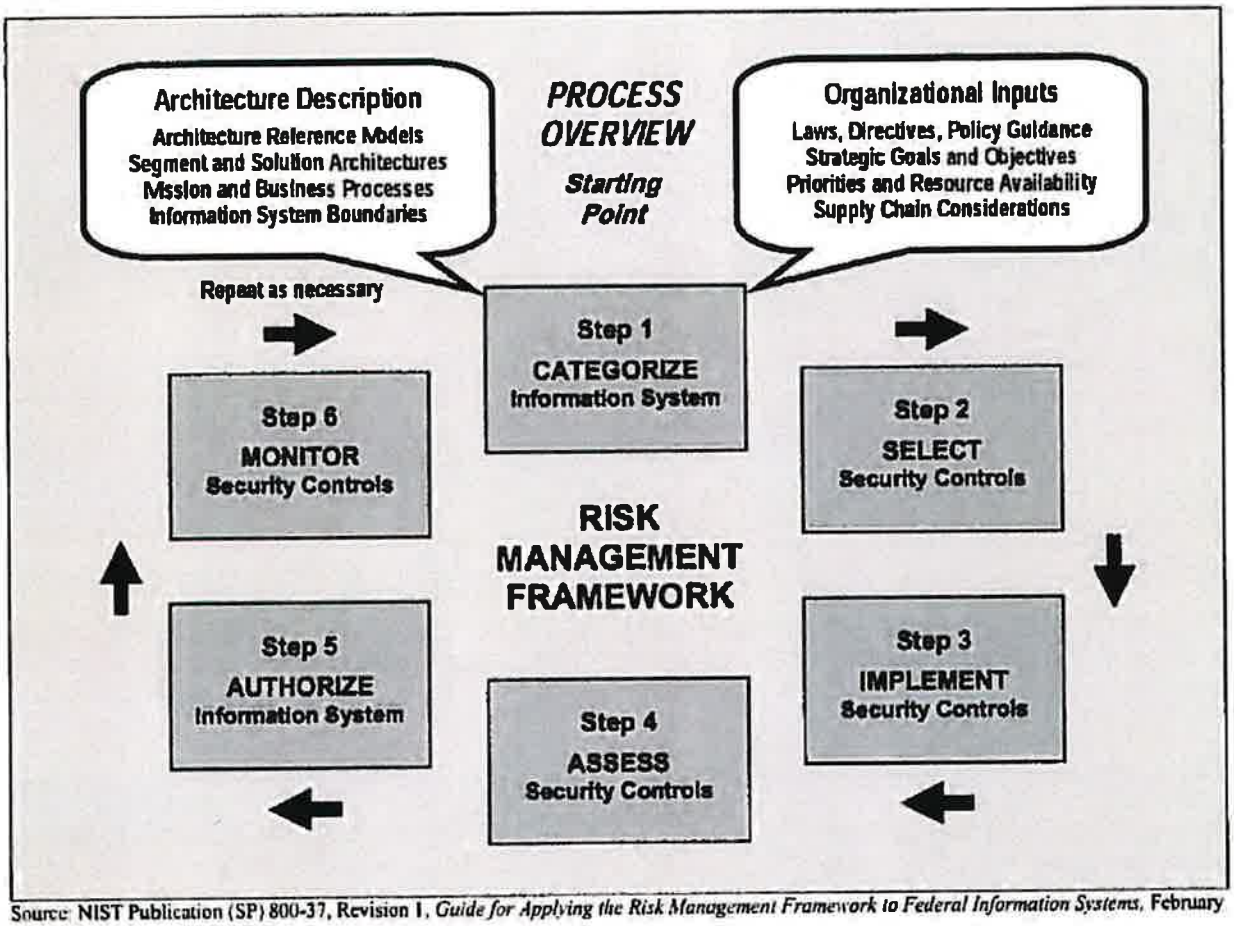
We also performed testing to determine the adequacy of controls surrounding POBITS. During the scope of our testing, the server vendor released 126 patches for the server hosting POBITS. We selected a non-statistical sample of 45 patches to determine if USCP correctly applied the patch.

Furthermore, we performed testing to determine the adequacy of controls surrounding the VPN portal. We reviewed documentation to ensure that the Department had established a configuration baseline and monitored system configurations against the approved baseline. We also performed limited authentication testing to verify the use of two-factor authentication. In addition, we tested whether administrator access to the VPN portal was restricted based on job responsibility.

A risk management framework (RMF) is required for executive branch agencies. Because it is a legislative branch entity, the Department does not have a mandated RMF. An RMF is the unified information security framework for the entire Federal Government that is replacing the legacy Certification and Accreditation (C&A) processes within departments and agencies. In the absence of a required RMF, we used the National Institute of Standards and Technology (NIST) RMF as criteria for performing our audit work. NIST considers the framework to be an IT and security best practice. According to OIG-2015-10 *Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program*, dated September 2015, USCP officials intend to adopt the NIST RMF as shown in Exhibit 1. In an October 28, 2015 response to the OIG report, the Department stated:

> The Chief Information Security Officer (CISO) determined that the Department will follow NIST SP 800-37 rev1, *Guide for Applying the Risk Management Framework to Federal Information Systems.* Additionally, the CISO is in the process of developing several Directives and Standard Operating Procedures to address all the policies and procedures within the Office of Information Systems (OIS). This will be a complete and thorough process, and we expect to have the entire review published and implemented by September 2016.

Exhibit 1 – NIST Risk Management Framework



Source: NIST Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.

OIG conducted this performance audit in Washington, D.C., from October 2015 through February 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 February 10, 2016, we provided a draft copy of this report to Department officials for comment. On February 10, 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.

RESULTS

Overall, the Department did not have adequate internal controls and processes for ensuring security for Web site applications as well as efficient and effective operations. In addition, the Department did not have policies or procedures in place for the use of public Web site applications. Furthermore,

the privacy policy on the USCP Web site referred to the Department of Homeland Security (DHS) Web site in instances where it should have referred to the USCP Web site.

Inadequate Controls

The Department did not have adequate controls in place that would help ensure the integrity of the USCP Web site and Web applications with public access. Examples of inadequate controls or lack of appropriate actions include the following:

- USCP did not prepare Plan of Action and Milestones (POA&Ms) [redacted] A POA&M is a tool identifying actions needed to address a security vulnerability.

- USCP did not adequately monitor third parties as evidenced by the lack of evidence of an agreement between USCP and GPO regarding GPO's hosting of USCP's Web site and the lack of a Statement on Standards for Attestation Engagements Number 16 report, or similar report, to validate controls performed by GPO.

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- USCP did not have System Security Plans (or equivalent documentation) detailing categorization of the public Web site and Web applications and selected baseline of security controls.

- USCP could not provide documentation of an approved configuration baseline for POBITS infrastructure.

- [redacted]

In all likelihood, the Department would have prevented many of the internal control weaknesses identified during the audit if it had fully adopted an RMF. In its OIG-2015-10 audit, OIG recommended that the Department adopt an RMF, and the Department indicated that it intended to adopt the NIST RMF. As of February 2016, OIS continues with its efforts to implement the NIST RMF. According to an OIS official, adopting an RMF is a time-consuming process.

[redacted]

The Department did not have a well-documented or easily understood RMF with corresponding policies and procedures, as recommended by best practices and NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* dated February 2010. As a result, the Web site and Web application security processes that we observed were not repeatable or consistently implemented. For example, OIS was performing vulnerability scanning of POBITS. However, we were unable to obtain evidence that OIS was consistently addressing the results of the scanning, which is a necessary part of a well-designed information security program. Before it can begin implementing specific information security practices for the Web, the Department must have a framework to guide structure.

An effective risk management program ensures that the agency has assessed its policies and procedures as well as verified that all is functioning as intended. An effective program also provides a process for management to consider the importance of systems, identify and implement controls around those systems, assess those controls, and ultimately identify and remediate any risks around the systems. Management has designed some of its processes around the NIST Revision 1 guidance but must still perform significant work to achieve full implementation.

According to NIST SP 800-37, Revision 1, a well-developed RMF framework would include the following:

- **Categorize** the information systems and the information processed, stored, and transmitted by the system based on an impact analysis.
- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organization, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Conclusions

The Department did not have adequate controls in place that would ensure the integrity of the USCP Web site and public Web applications. Without an overarching RMF, the USCP system of internal controls, particularly those for information security, cannot be effective or sustainable. We therefore, repeat the following recommendation from report OIG-2015-10, *Performance Audit of the*

United States Capitol Police's Fiscal Year 2015 Information Security Program, dated September 2015:

> **Recommendation 1: We recommend that the United States Capitol Police assign an appropriate official to (1) identify an appropriate risk management framework to implement Department-wide and (2) develop policies and procedures to implement the chosen risk management framework.**

Noncompliance With and Lack of Policies and Procedures

USCP did not always comply with its policies and procedures. For example, password policy requires that each quarter OIS must change passwords for system-level administrator accounts. Instead, passwords for the VPN portal were changed every 6 months. In addition, no policies or procedures existed for the security of Web-based applications.

Noncompliance with Policies and Procedures

[redacted] OIS informed us that they have not considered the account to be a [redacted] in the past. They also indicated that OIS would comply with the 3-month policy in the future.

Lack of Policies and Procedures

The Department did not develop policies and procedures for public Web applications. Although USCP Directive [redacted], dated February 3, 2014, addresses the public-facing Web sites and the internal PoliceNet Intranet sites, OIS did not have policies or procedures related to public Web applications such as the VPN portal or POBITS. Policies and procedures for public Web applications are necessary to ensure that the day-to-day activities of the staff follow a rigorous, repeatable process. Once fully developed and approved, USCP should then use the RMF as guidance in identifying the policies and procedures it will need to develop and implement a strong Web application security program.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, Section 2.2.5, *Information Security Policy and Guidance*, dated October 2006, states:

> Information security policy is an essential component of information security governance – without the policy, governance has no substance and rules to enforce. Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal agency requirements.

Conclusions

USCP did not comply with Department policies and procedures regarding passwords for system administrator accounts. The Department also lacked written policies and procedures related to public Web applications. Without an effective body of policies and procedures, employees do not have the appropriate information for reliably and consistently performing their duties, which ultimately weakens the overall public Web application security program. We, therefore, make the following recommendations:

Recommendation 2: We recommend that the United States Capitol Police provide management oversight of the staff responsible for password management. Staff should be apprised of the United States Capitol Police policies and procedures and follow the guidance on a consistent basis.

Recommendation 3: We recommend that the United States Capitol Police develop policies and procedures for public Web site applications.

Areas for Improvement

Opportunities exist for the Department to improve its public Web site. During review of the USCP Web site privacy policy, we noted that the policy made several references to DHS. For example, the privacy policy stated, "When you browse, read pages or download information on The Department of Homeland Security's websites, we automatically gather and store certain technical information about your visit." According to USCP officials, the policy should have referenced USCP rather than DHS. As of February 26, 2016, the Department had corrected the references to DHS.

We also noted that the privacy policy on the USCP Web site did not contain several elements required by the Federal Information Security Management Act (FISMA) of 2002. FISMA Section 208, *Privacy Provisions*, states:

> (1) Privacy Policy on Web sites—
>
> (A) Guidelines for Notices—The Director shall develop guidance for privacy notices on agency Web sites used by the public.
>
> (B) Contents—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
>
> (i) what information is to be collected;
>
> (ii) why the information is being collected;
>
> (iii) the intended use of the agency of the information;
>
> (iv) with whom the information will be shared;

> (v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
>
> (vi) how the information will be secured; and
>
> (vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the "Privacy Act"), and other laws relevant to the protection of the privacy of an individual.

Privacy policy for USCP, however, did not include the following elements that FISMA requires.

- With whom any information that is collected will be shared
- How information collected for site visitors is secure
- Other laws (if applicable) that are relevant to the protection of the privacy of the individual

Because USCP is a legislative-branch entity, it is exempt from many of the laws and regulations, such as FISMA, that apply to executive-branch agencies; however, these laws and regulations represent appropriate guidance and industry best practices.

Conclusions

Opportunities exist for the Department to improve its public Web site. USCP could also enhance its Web site by ensuring that the privacy policy on the public Web site complies with the requirements of FISMA.

> **Recommendation 4: We recommend that the United States Capitol Police revise the privacy policy posted on the public Web site. The policy should remove any inaccuracies and be updated to include all the relevant criteria the Federal Information Security Management Act (2002) requires.**

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police assign an appropriate official to (1) identify an appropriate risk management framework to implement Department-wide and (2) develop policies and procedures to implement the chosen risk management framework.

Recommendation 2: We recommend that the United States Capitol Police provide management oversight of the staff responsible for password management. Staff should be apprised of the United States Capitol Police policies and procedures and follow the guidance on a consistent basis.

Recommendation 3: We recommend that the United States Capitol Police develop policies and procedures for public Web site applications.

Recommendation 4: We recommend that the United States Capitol Police revise the privacy policy posted on the public Web site. The policy should remove any inaccuracies and be updated to include all the relevant criteria the Federal Information Security Management Act (2002) requires.

DEPARTMENT COMMENTS

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

February 26, 2016

COP 160176

MEMORANDUM

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

FROM: Kim C. Dine
Chief of Police

SUBJECT: Response to Office of Inspector General (OIG) draft report *Performance Audit of the United States Capitol Police Public Web Site and Web Applications* (Report No. OIG-2016-05).

The purpose of this memorandum is to provide the United States Capitol Police's response to the recommendations contained within the Office of the Inspector General's draft report *Performance Audit of the United States Capitol Police Public Web Site and Web Applications* (Report No. OIG-2016-05).

The Department agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon policies and procedures. The Department will assign Action Plans to appropriate personnel regarding each recommendation 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,

Kim C. Dine
Chief of Police

cc: Matthew R. Verderosa, Assistant Chief of Police
Richard L. Braddock, Chief Administrative Officer
[redacted], USCP Audit Liaison

[redacted]

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 at:
United States Capitol Police
Attn: Office of Inspector General, Investigations
119 D Street, NE
Washington, DC 20510

Or visit us – we are located at:
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