UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program

Report Number OIG-2015-10

September 2015

~~REPORT RESTRICTION LANGUAGE~~

~~IMPORTANT NOTICE~~

~~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.~~

Cotton & Company
Answers Questioned

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

September 28, 2015

Fay Ropella
Inspector General
Office of Inspector General
U.S. Capitol Police

Subject: Report on the FY 2015 Performance Audit of the U.S. Capitol Police's Information Security Program

Dear Ms. Ropella,

Cotton & Company LLP is pleased to submit this performance audit report of the United States Capitol Police's (USCP) information security program. We conducted an independent performance audit of the USCP's information security program as of March 27, 2015. Cotton & Company performed the work from March through August 2015.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Sincerely,
Cotton & Company LLP

Loren F. Schwartz, CPA, CISSP, CISA
Partner, Information Assurance

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

Chief Information Officer	CIO
Chief Information Security Officer	CISO
Construction Security Division	CSD
Deputy Chief Administrative Officer	DCAO
Federal Information Processing Standards	FIPS
Federal Information Security Management Act/Federal Information Security Modernization Act	FISMA
Fiscal Year	FY
Information Technology	IT
National Institute of Standards and Technology	NIST
Office of Information Services	OIS
Office of Inspector General	OIG
Office of Management and Budget	OMB
Physical Security Division	PSD
Plans of Action and Milestones	POA&Ms
Project Planning Section	PPS
Risk Management Framework	RMF
Security Coordination Section	SCS
Security Equipment Section	SES
Security Services Bureau	SSB
Special Publication	SP
Security Operations Section	SOS
System Security Plan	SSP
Technical Countermeasures Division	TCD
United States Capitol Police	USCP or Department

EXECUTIVE SUMMARY

In accordance with our annual plan, the United States Capitol Police (USCP or the Department) Office of Inspector General (OIG) engaged Cotton & Company LLP to conduct an independent performance audit of USCP's information security program. Our audit focused on two overarching areas: The Department's current vulnerability management practices and its cyber security framework and risk management processes. We considered policies, procedures, and processes for both the USCP Office of Information Services (OIS) and the Security Services Bureau (SSB) as of March 27, 2015. We also considered the eight information security priority topics that the Office of Management and Budget (OMB) communicated to executive-branch agencies. Those eight topics, as applied to USCP, were:

- The manner in which USCP protects data, [redacted]
- Actions USCP has taken to improve its situational awareness.
- USCP's ability to increase its cybersecurity proficiency.
- USCP's overall risk awareness.
- USCP's standard and automated processes.
- USCP's ability to control, contain, and recover from incidents.
- The manner in which USCP ensures security throughout the information system life cycle.
- The manner in which USCP considers and reduces its attack surfaces.

While OIS and SSB appeared to be executing some day-to-day information technology and security practices, we identified several significant weaknesses in its overall approach to information security. Specifically, OIS and SSB did not have:

- An overarching governance and risk management process that allows for proactive decision-making related to information security.
- Comprehensive policies and detailed procedures to allow for repeatable, reliable information security processes.
- An established mechanism to inform senior management of USCP's current risk posture as it relates to information security.
- A centralized approach to information security, which hampers its ability to effectively implement a comprehensive program. USCP OIG previously reported this finding in a December 2011 performance audit report.[1]

USCP's information security program is managed by two small groups of well-intentioned professionals within OIS and SSB. However, without a risk management framework,

1 *Audit of United States Capitol Police Enterprise Architecture*, Report Number OIG-2012-01, dated December 2011.

documented policies and procedures, and significantly more senior management attention, the integrity, availability, and confidentiality of USCP information systems and data are at risk.

USCP is a relatively small federal agency and appears to have an organizational structure that would support more centralized oversight of its information security program. OIS has drafted an information security program plan, while SSB is still in the very early stages of formalizing an information security plan. Both OIS and SSB are in a similar position of maturity as it relates to building out their information security programs, and both indicated that they required more resources to fully implement their information security programs as intended. Having two units within USCP seeking to achieve similar goals, undergoing similar processes, and potentially acquiring similar tools and technologies in a decentralized manner appears to be an inefficient use of resources.

As noted above, USCP is performing well in certain areas of information security. For example, we obtained evidence indicating that both SSB and OIS conduct regularly scheduled and managed vulnerability scanning. The SSB environment is segregated from the remainder of the OIS environment and from other external networks, which enables SSB to mitigate potential vulnerabilities. While these positive efforts help mitigate the risk to USCP's information security program, the Department should take immediate action to begin addressing the four overarching conditions noted above. Implementing an effective information security program will not be an easy or quick process, and it will require significant attention and support from USCP senior management. As a first step in this process, the Acting Chief Information Officer stated that the Department will use year-end funding to augment an existing contract to obtain additional assistance in documenting information security policies. This process will begin shortly.

We present our findings in order of risk, from highest to lowest. A complete list of OIG recommendations is shown in Appendix A. OIG provided a draft report for comment on September 18, 2015, and conducted an exit conference with Department officials on September 28, 2015. We incorporated the Department's comments as applicable and attached the Department's response to the report in its entirety in Appendix B.

Background

The United States Capitol Police (USCP or the Department) is a law enforcement agency within the legislative branch of the U.S Government. It is tasked with protecting the Capitol Complex and the members of the United States Congress, both domestically and abroad. USCP's primary technology office, the Office of Information Services (OIS), provides enterprise-wide information technology (IT) solutions and supports a wide range of systems in use. In addition, the Security Services Bureau (SSB) maintains its own IT solutions and resources.

OIS is led by the Chief Information Officer (CIO), who reports to the Chief Administrative Officer via the Deputy Chief Administrative Officer (DCAO). The previous CIO resigned in

early 2015, and the DCAO is serving as the Acting CIO until USCP can identify a permanent replacement. The Chief Information Security Officer (CISO) reports directly to the Acting CIO.

SSB originated from a task force established by the Capitol Police Board in 1995. It provides physical and technical security for the Capitol Complex. Aligned under the Office of the Chief Operating Officer, SSB consists of three divisions: the Construction Security Division (CSD), the Physical Security Division (PSD), and the Technical Countermeasures Division (TCD). As a main area of focus, PSD has four sections: the Project Planning Section (PPS), the Security Equipment Section (SES), the Security Coordination Section (SCS), and the System Operations Section (SOS).

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 IT that support operations and assets.

Objective(s), Scope, and Methodology

The USCP Office of Inspector General (OIG) engaged Cotton & Company LLP to conduct an independent performance audit of USCP's information security program. Our objective was to assess the effectiveness of USCP's information security program. Specifically, we:

1. Assessed USCP's current vulnerability management practices.
2. Reviewed USCP's cyber security framework and risk management processes.
3. Assessed the eight Office of Management and Budget (OMB) information security priority topics as applied to USCP, including:

    - The manner in which USCP protects data, [redacted]
    - Actions USCP has taken to improve its situational awareness.
    - USCP's ability to increase its cybersecurity proficiency.
    - USCP's overall risk awareness.
    - USCP's standard and automated processes.
    - USCP's ability to control, contain, and recover from incidents.

- The manner in which USCP ensures security throughout the information system life cycle.
- The manner in which USCP considers and reduces its attack surfaces.

Our audit focused on the following USCP organizations:

- OIS, which provides policy, planning, budgeting, design, testing, implementation, and management of USCP's automated information and IT.

- SSB, which is responsible for supervising and delivering security surveys of congressional offices, providing potential locations for the storage of national security information, designing and maintaining physical security systems, and providing technical security countermeasure inspections.

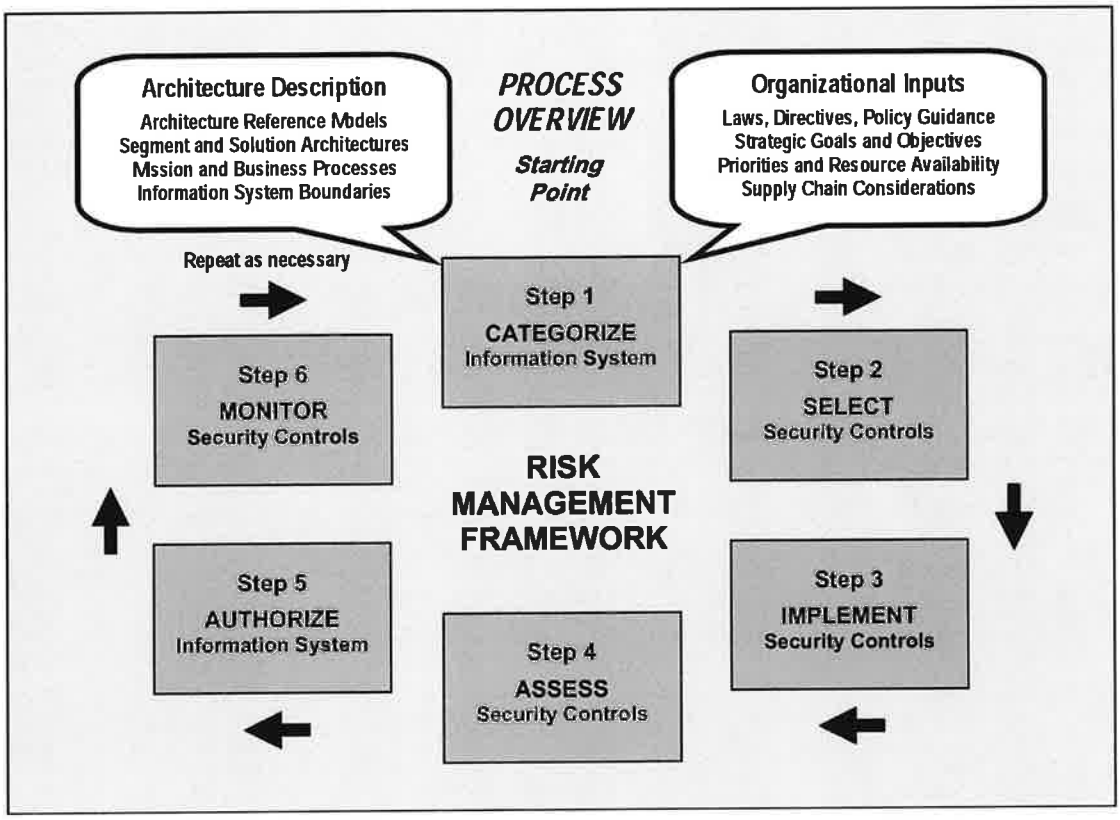
Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management officials on September 17, 2015, and included their comments where appropriate.

To accomplish our audit objective, Cotton & Company interviewed USCP personnel and reviewed documentation related to USCP's information security program, such as security policies and procedures, system security plans (SSPs), assessment and authorization documentation, disaster recovery plans, system documentation and outputs, and incident reports. We reviewed system processes to determine the adequacy and effectiveness of selected controls. We also reviewed system plans of action and milestones (POA&Ms) to identify controls in scope that management had already determined were not in place. We followed up with management to confirm control deficiencies noted and, if management confirmed the deficiencies, did not perform additional testing. We also inquired regarding the eight OMB information security priority topics and, where possible, performed additional testing on these topics.

USCP is a legislative-branch entity and therefore does not have a mandated risk management framework (RMF). In the absence of a required RMF, we used the National Institute of Standards and Technology (NIST) RMF as criteria in performing our audit work. This framework is required for executive-branch agencies and is considered an IT and security best practice. In our meetings with USCP, the agency indicated that it intends to adopt the NIST RMF.

The NIST RMF is depicted in Exhibit 1.

Exhibit 1 – NIST Risk Management Framework



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

OIG provided a draft copy of this report to Department officials for comment on September 18, 2015, and conducted an exit conference with Department officials on September 28, 2015. We incorporated the Department's comments as applicable and attached the Department's response to the report in its entirety as Appendix B.

Results

New cyber threats emerge on a daily basis, and the evolving nature of these threats is challenging government institutions to re-evaluate how they manage the security of their systems and data. Failure to adequately secure and monitor IT assets can lead to significant damages and potentially threaten national security. While USCP appears to be executing some day-to-day IT and security practices, we identified several significant weaknesses in its overall approach to information security. Specifically, we identified the following areas for improvement:

- USCP has not fully implemented the NIST RMF in its information security program.
- USCP has not developed and implemented comprehensive policies and detailed procedures to allow for repeatable, reliable information security processes.

- USCP does not have an established mechanism for informing stakeholders of the agency's information security risk posture.
- USCP's information security program is decentralized.

Overall Risk Management Framework Needed

USCP is a legislative-branch entity and therefore does not have a mandated RMF. In the absence of a required RMF, we used the NIST RMF as criteria in performing our audit work. This framework is required for executive-branch agencies and is considered an IT and security best practice. In our meetings with USCP, the agency indicated that it intends to adopt the NIST RMF.

USCP's information security program does not include a well-documented and well-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*. As a result, the information security processes that we observed were neither repeatable nor consistently implemented. For example, we obtained strong evidence that USCP was performing vulnerability scanning; however, we were unable to obtain evidence that USCP was consistently addressing the results of the scanning, which is a necessary part of a well-designed information security program. Before USCP management can begin implementing specific information security practices, it must have a framework to guide the organization.

An effective risk management program ensures that the organization has assessed its policies and procedures and verified that they are working as intended. It 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 risks around the systems. As noted, NIST has developed an RMF, described in NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.* USCP management has designed some of its processes around this RMF but still must perform significant work to achieve full implementation.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010, states:

- **Categorize** the information system and the information processed, stored, and transmitted by that 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 organizations, 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.

Without an overarching RMF, USCP's system of internal controls, particularly around information security, cannot be effective or sustainable. Thus, we make the following recommendation:

> **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.**

Lack of Comprehensive Policies and Procedures

Neither OIS nor SSB has fully developed and implemented comprehensive policies and detailed procedures to allow for repeatable, reliable information security processes. Such policies and procedures are the next core piece of a well-designed and well-implemented information security program once an organization has developed an RMF. Both OIS and SSB have started developing, documenting, and implementing many elements of an information security program, including creating policies and procedures; however, much work still remains. For example, neither OIS nor SSB has created detailed policies and procedures regarding:

- Vulnerability Management
  - Confirming vulnerabilities and performing vulnerability tracking and aging
  - Performing timely remediation of prioritized vulnerabilities
  - Scanning for potential rogue wireless access devices within the network
- Configuration Management
  - Monitoring against approved baselines
  - Establishing remediation timelines for deviations against baselines

Policies and procedures in these and many other areas are necessary to ensure that the day-to-day activities of the information security staff and the remainder of USCP are well-understood and follow a rigorous, repeatable process. As noted above, USCP's first step in establishing an information security program must be to implement an RMF. USCP should then use this RMF as guidance in identifying the policies and procedures that it will need to develop and implement in order to support a strong information security program.

Information security includes preventive controls to stop security incidents from occurring, as well as processes for detecting and responding to such incidents if they do occur. All of these

processes should be governed by policies and procedures. USCP has some elements of good policy, and it has detailed procedures in some areas. In addition, the Acting CIO stated that the Department will use year-end funding to augment an existing contract to obtain additional support in documenting information security policies. However, many pieces of the information security program are currently lacking this critical oversight.

NIST SP 800-100, *The 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.
>
> Agency information security policy should address the fundamentals of agency information security governance structure, including:
>
> - Information security roles and responsibilities;
> - Statement of security controls baseline and rules for exceeding the baseline; and
> - Rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance.
>
> Supporting guidance and procedures on how to effectively implement specific controls across the enterprise should be developed to augment an agency's security policy.

Without an effective body of policies and procedures, employees will not have the information to reliably and consistently perform their duties, thereby weakening the overall information security program. Thus, we make the following recommendation.

> **Recommendation 2: We recommend that the United States Capitol Police assign an appropriate official to (1) identify the information security policies and corresponding procedures necessary to support the information security program Department-wide, (2) develop the identified policies and corresponding procedures, and (3) implement the finalized policies and procedures.**

No Mechanism for Informing Stakeholders of Information Security Risk Posture

Neither OIS nor SSB had an established mechanism for regularly informing senior management of the current risk posture of USCP's information security program. Information security issues abound in the media today, and the risks and uncertainties around information security have reached the attention of the highest levels of senior management, both in publicly traded corporations and in federal agencies. A well-developed information security program ensures that senior management understands the agency's risk posture and is regularly briefed on the status of the program. The Acting CIO and the DCAO stated that the CISO communicates with OIS senior management only on an as-needed basis; i.e., when there is an information security event or concern. An effective information security program receives focus and

attention from the most senior levels of management to ensure that the agency is proactively managing its information security.

NIST SP 800-100, *The Information Security Handbook, A Guide for Managers*, Section 2.2.3, *Key Governance Roles and Responsibilities*, Subsection 2.2.3.1, *Agency Head*, dated October 2006, states:

> The Clinger-Cohen Act assigns the responsibility for ensuring "that the information security policies, procedures, and practices of the executive agency are adequate." FISMA provides the following details on agency head responsibilities for information security:
>
> - Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
> - Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;
> - Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission;
> - Ensuring that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control;
> - Designating a CIO and delegating authority to that individual to ensure compliance with applicable information security requirements;
> - Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and
> - Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.

The Department (i.e., OIS and SSB) cannot fulfill its information security responsibilities without senior management involvement in the information security program, and USCP senior management officials will not be aware of information security risks to agency operations. Thus, we make the following recommendation.

> **Recommendation 3: We recommend that the United States Capitol Police develop (1) a process to ensure that the Department senior management, including the Chief of Police, is regularly informed about the status of the information security program and (2) measurable key security metrics to report to senior management on a regular basis.**

Decentralized Information Security Program

USCP's information security program is decentralized, with both OIS and SSB responsible for aspects of the program. This further hampers the Department's ability to effectively implement a comprehensive security program.

USCP's IT management is also decentralized, with OIS and SSB both maintaining separate IT groups. SSB explained that this is because its operational security environment is different from OIS's [redacted] While we understand the need to have different protections and information security controls over different IT systems and environments, having two different organizations running parallel processes is an inefficient use of resources. For example, it is inefficient for two different organizations to both perform the same vulnerability scans. In addition, both organizations indicated that they were working to update policies and procedures around similar topical areas.

The NIST RMF is a scalable framework that can address a full range of information systems, from low-risk and less-sophisticated systems all the way to the most complex and highly sensitive systems. We concluded that USCP may be able to gain efficiencies in its use of resources by establishing a common framework for both organizations. This would enable SSB to continue implementing more tightly constrained controls around its secure environment while still allowing OIS to have more flexibility in its operating environment, and USCP would reap the benefits of maintaining a single set of guiding principles.

NIST SP 800-100, *The Information Security Handbook: A Guide for Managers*, Section 2.2.2, *Information Security Governance Structures* states:

> Agencies in the process of establishing or changing their information security governance structure should consider the following key factors to determine the optimal extent of the centralization or decentralization:
>
> - Agency size;
> - Agency mission and its level of diversification or homogeneity;
> - Existing agency IT infrastructure;
> - Existing federal and internal governance requirements;
> - Size of agency budget;
> - Agency information security capabilities;
> - Number of, and distance between, physical locations; and
> - Decision-making practices and desired rate of change in information security practices.

Thus, we make the following recommendation.

> **Recommendation 4: We recommend that the United States Capitol Police assess whether it is viable and productive to place the Office of Information Services and Security Services Bureau information security resources under a common management oversight.**

APPENDICES

Listing 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 assign an appropriate official to (1) identify the information security policies and corresponding procedures necessary to support the information security program Department-wide, (2) develop the identified policies and corresponding procedures, and (3) implement the finalized policies and procedures.

Recommendation 3: We recommend that the United States Capitol Police develop (1) a process to ensure that the Department senior management, including the Chief of Police, is regularly informed about the status of the information security program and (2) measurable key security metrics to report to senior management on a regular basis.

Recommendation 4: We recommend that the United States Capitol Police assess whether it is viable and productive to place the Office of Information Services and Security Services Bureau information security resources under a common management oversight.

Department Comments

Phone: 202-224-9806

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

September 23, 2015

COP 151138

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's Fiscal Year 2015 Information Security Program* (Report No. OIG-2015-10).

The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of the Inspector General's (OIG's) draft report *Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program (*Report No. OIG-2015-10).

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 in effect to achieve long term resolution of these matters.

Thank you for the opportunity to respond to the OIG's draft report. Your continued support of the men and women 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

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
INSPECTOR GENERAL