



UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL

Audit of USCP Privacy Program

Report Number OIG-2009-03

March 2009

~~Important Notice: Distribution of This Document Is Restricted~~

~~This report is intended solely for the official use of the United States Capitol Police or the Capitol Police Board, or any agency or organization receiving a copy 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 the Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~



UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003

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 audit, reviews, and investigative and special reports prepared by OIG periodically as part of its oversight responsibility with the respect to the United States Capitol Police 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 a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

Carl W. Hoccker

Carl W. Hoccker
Inspector General

TABLE OF CONTENTS

	<u>Page</u>
Abbreviations	3
Executive Summary	4
Background	5
Objective, Scope, and Methodology	6
Results	7
Privacy Policies and Procedures Have Not Been Developed and Implemented	8
The Department Has Not Identified All Personally Identifiable Information	9
A Privacy Awareness Training Program Has Not Been Implemented	10
Appendices	11
Appendix A – Summary of Recommendations	12
Appendix B – Department Comments	13

Abbreviations

Chief Privacy Officer	CPO
Federal Information Security Management Act of 2002	FISMA
Fiscal Year	FY
Office of Information Systems	OIS
Office of Inspector General	OIG
Office of Management and Budget	OMB
Personally Identifiable Information	PII
Privacy Board	Board
Sensitive Health Information	SHI
United States Capitol Police	USCP or Department
The Privacy Act	The Act

EXECUTIVE SUMMARY

In accordance with our Fiscal Year (FY) 2009 annual plan, the Office of Inspector General (OIG) conducted an audit to determine whether (1) the United States Capitol Police (USCP or Department) had developed a privacy program that adheres to federal standards and best practices and (2) the program safeguards assisted the Department in protecting stakeholder information from potential disclosure, specifically those of Congressional members and their staff. Our scope included the Department's privacy program(s) in effect as of October 1, 2008.

While the Department, as a legislative branch agency, is not required to comply with the Federal Privacy Act¹ (the Act) of 1974 and the Office of Management and Budget (OMB) guidance, the Department used these principles as best practices in the development of its policies and procedures. The Act, Federal Information Security Management Act of 2002 (FISMA)², and OMB memos require each Federal agency to:

1. Develop and implement policies and procedures for an overall privacy program.
2. Identify and safeguard personally identifiable information (PII) in both paper and electronic form.
3. Develop a training program to annually educate employees on the requirements for handling PII.
4. Perform risk assessments over major information systems and implement appropriate safeguards based on those risks.
5. Implement secure baseline configurations over information systems.

The Department does not have a privacy program in place to ensure that privacy related risks have been identified and adequately addressed. While the Department does collect and handle PII of Congressional members and their staff, the Department has not identified where PII is collected, maintained, processed, or disseminated. The Department has neither clearly defined the roles and responsibilities of key privacy personnel nor provided applicable training to such personnel. We also noted USCP's organizational chart did not identify the Chief Privacy Officer (CPO) or include this position within its organizational structure. Additionally, the role of the CPO has not yet been defined by the Department. The lack of a CPO position on the organization chart and the absence of a clear role for the CPO indicates that the position's authority has not been communicated or recognized within the Department.

During the course of our interviews and documentation reviews, no instances of either intentional or inadvertent releases of PII came to our attention. However, the scope of our audit was not designed to identify all breaches of PII.

¹ 5 U.S.C § 552a.

² Title III of the E-Government Act of 2002, Pub. L. 107-347.

The Department appointed a CPO in August 2007. The Department also established a Privacy Board (Board) consisting of the CPO and other key personnel. The Board's overall objective is to "Determine appropriate policy, procedures, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other Privacy-related matters." While the Board has taken some action to address privacy concerns, the majority of actions taken at the time of our audit were still in the draft or initial stages and therefore not functioning effectively.

To improve the internal efficiency and effectiveness of its PII program and to assist in safeguarding stakeholder information, OIG is recommending that the Department finalize its policies and procedures; clearly define roles, responsibilities, and authorities of the CPO and other key privacy personnel; and provide applicable privacy training to all contractors and employees. Most importantly, the Department should develop and implement procedures to identify and safeguard PII holdings within the organization. A listing of all OIG recommendations is shown in Appendix A.

By collecting only the necessary PII and managing it properly, the Department can reduce the volume of PII they possess, which in turn reduces the risk to the Department and the burden of safeguarding such information. Given the serious lapses in protection of PII affecting numerous Federal agencies over the last several years, it is important to be aware and mindful of the responsibilities each employee has to protect and secure the information entrusted to the Department in their professional responsibilities.

On March 19, 2009, OIG conducted an exit conference with Department officials and provided a draft report for comment. We incorporated the Department's comments as applicable and attached their response to the report in its entirety in Appendix B.

BACKGROUND

Although not required to follow executive branch guidance, USCP has opted to follow as best practices, the Act, FISMA, and OMB guidance in the development of its policies and procedures.

The Act of 1974 set forth a series of requirements governing Federal agency personal record-keeping practices. The Act not only places the principal responsibility for compliance with its provisions on Federal agencies but also provides that OMB develop guidelines and regulations, as well as provide continuing assistance to and oversight of the implementation of the operative provisions of the Act. OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, reemphasizes the many responsibilities under law and policy to appropriately safeguard sensitive PII. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, identifies the term "personally identifiable information" as information that can be used to distinguish or trace an individual identity, such as their name, social security number, biometric records, etc. alone, or when combined with other

personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

USCP's Office of Information Systems (OIS), Draft Policy & Procedure Manual, [REDACTED] refers to the following information as sensitive personally identifiable information (Sensitive PII):

1. An individual's social security number alone; or
2. An individual's name or address or phone number in combination with one or more of the following: date of birth, social security number, driver's license number or other state identification number, or foreign country equivalent; passport number, financial account numbers, credit or debit card numbers.

Sensitive Health Information (SHI) includes medical records and other individually identifiable health information, whether on paper, in electronic form, or communicated orally. SHI related to the past, present, or future physical or mental health or condition or an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Nonpublic Information includes generally all non-law enforcement documents collected, generated or maintained by the Department. "Nonpublic" will normally cover many or most of the documents Department staff work with internally on a day-to-day basis.

The CPO position was established in August 2007. However, roles and responsibilities for the CPO have not yet been clearly established. The CPO is the Director of the Office of Information Systems (OIS). According to the undated Draft Privacy Board Charter, members of the Board will be appointed by the CPO. The Board, according to its charter, is required to meet at least quarterly.

OBJECTIVE, SCOPE, AND METHODOLOGY

On behalf of the OIG, Cotton & Company LLP performed an audit of the Department's privacy program to determine whether (1) USCP had developed a privacy program that adheres to federal standards and best practices and (2) the program safeguards assisted the Department in protecting stakeholder information from potential disclosure, specifically those of Congressional members and their staff. Our scope included the Department's privacy program(s) in effect as of October 1, 2008.

To accomplish our objective, we reviewed USCP operational and program data and applicable Federal laws and Department directives; written policies; and interviewed 23 sworn and civilian officials related to its privacy program. In addition, to gain a better understanding of how the Department collects, processes, stores, and protects privacy information, we also developed a questionnaire and surveyed sworn and civilian employees. We developed the questionnaire to

assist in determining the general awareness among USCP personnel concerning privacy policies, procedures, and practices. From the Department's Pay Cap report, dated October 16, 2008, we judgmentally selected 315 sworn and civilian employees from all administrative and operational areas of the Department to complete the questionnaire. Ninety-eight employees completed and returned the questionnaire resulting in a response rate of about 31 percent.

Furthermore, we reviewed draft privacy policies and procedures that management developed in FY 2008. These privacy policies and procedures included:

- October 21, 2008, Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]
- Undated Draft [REDACTED]

For this audit we drew upon Federal privacy laws and regulations, including the Act, FISMA, and privacy specific OMB memos as industry best practice audit criteria.

We conducted fieldwork in Washington, D.C., from December 2008 through February 2009. We 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. On March 19, 2009, we conducted an exit conference with Department officials and incorporated applicable comments. We attached their response in its entirety in Appendix B.

RESULTS

Overall, the Department does not have a privacy program to ensure privacy related risks have been identified and adequately addressed. Specifically, the Department has not fully developed and implemented privacy policies and procedures. The Department also has not identified PII holdings within the organization. Furthermore, the Department has not established and implemented a privacy training program, which clearly informs its employees and contractors about privacy risks and their responsibilities related to safeguarding sensitive PII. As a result, the Department is at an increased risk that a privacy breach could occur. Safeguarding PII in the possession of the

Department and preventing its breach are essential to ensure the government retains the trust of its employees, Congress, and the American public. Recognizing that safeguarding against breaches has greater value than responding to breaches when they occur.

Privacy Policies and Procedures Have Not Been Developed and Implemented

The Department has not fully developed, implemented, and distributed to Department personnel its privacy policies and procedures. As a result, controls are not adequate to ensure privacy policies and procedures have been documented and implemented in order to safeguard stakeholder information from potential disclosure. Specifically, the Department has developed a number of privacy policies and procedures; however, these documents are currently in draft. Our review of these draft documents noted the following:

- The Department had not clearly documented privacy roles and responsibilities. Policies should clearly document responsibilities of individuals, by position, involved in developing, administering, and enforcing a privacy program.
- The Department had not identified privacy specific knowledge and training requirements for key personnel involved in administering its privacy program.
- According to the CPO, during the first quarter of FY 2009, the Department's privacy effort was temporarily suspended until the Department determines whether the privacy program will encompass administrative and law enforcement operations, or only administrative operations. As a result, the CPO's roles and responsibilities have not been clearly defined and the CPO role has not been reflected in the organizational chart.

OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, states:

As you know, the loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse.

This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area. In particular, the Privacy Act requires each agency to establish:

"rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance", and "appropriate administrative, technical and physical safeguards to insure the security and

confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."

Conclusions

The Department has not determined the scope of the privacy program and the CPO's role in the program. Therefore, the Department has not taken action on addressing privacy related risks. Specifically, draft documents did not clearly state the roles and responsibilities of key privacy personnel and did not identify specific knowledge and training requirements of such personnel. Additionally, the Department has not updated its organizational chart to identify the CPO and its position within the Department. Given the serious lapses in information security affecting numerous Federal agencies over the last several years, it is important to be aware and mindful of the responsibilities each of us has to protect and secure the information entrusted to us in our professional responsibilities. Thus, OIG is making the following recommendation.

Recommendation 1: We recommend that the United States Capitol Police finalize and fully implement a privacy program. The Department should clarify the Chief Privacy Officer's role and the position within the organization as well as include privacy policies and procedures. At a minimum, privacy policies and procedures should include:

- **Clear roles and responsibilities of key privacy personnel including the Chief Privacy Officer**
- **Privacy specific knowledge and training requirements for key personnel involved in administering the Department privacy program.**

The Department Has Not Identified All Personally Identifiable Information

The Department has not adequately identified where PII is collected, maintained, processed, or disseminated within the USCP. While no work has been performed, to date, to identify and document what PII the Department collects or handles, we did note that the Department has developed a draft questionnaire for individuals to fill out related to what information they handle. In addition, according to the CPO, the Department is looking into various automated tools to identify electronic PII stored in their systems. However, there is no timeline for dissemination of the questionnaire or acquisition of tools to assist in the identification of PII.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Section B, Privacy Requirements, states:

(1) Review and Reduce the Volume of Personally Identifiable Information a. Review Current Holdings, Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

Conclusions

Without identifying and documenting the types and locations of PII handled, the Department cannot be sure adequate safeguards have been put in place over sensitive PII. In addition, weak controls over sensitive PII could lead to the information being inappropriately accessed or released. Thus, OIG is making the following recommendation.

Recommendation 2: We recommend that the United States Capitol Police finalize draft documents related to identifying personally identifiable information that is collected or handled. Additionally, the Department should immediately conduct a review to identify where personally identifiable information is being collected, maintained, processed, or disseminated within the organization. This review should result in an inventory of the types, location, format (hard copy vs. electronic), and the accountable officials related to the personally identifiable information captured.

A Privacy Awareness Training Program Has Not Been Implemented

The Department does not have a privacy training program, which clearly informs its employees and contractors about privacy risks and their responsibilities related to safeguarding sensitive PII. While a training program is not in place, we did note that the Department has developed training materials. However, as of February 2009, the materials remained in draft and the Department had not developed a timeline for training its employees.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Section 2, Security Requirements (d. Train employees), states:

Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Conclusions

The Department has not established a formal privacy training program. Although the Department has developed materials for privacy training, the materials remained draft as of February 2009. Without a program to provide employees and contractors with periodic privacy training, the likelihood that those individuals will inappropriately handle or release sensitive PII increases. Thus, OIG is making the following recommendation.

Recommendation 3: We recommend that the United States Capitol Police finalize draft privacy training materials and require all employees and contractors to periodically complete privacy training (at least annually). In addition, management should track attendance of privacy training to ensure all individuals complete training in accordance with its established policy.

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police finalize and fully implement a privacy program. The Department should clarify the Chief Privacy Officer's role and the position within the organization as well as include privacy policies and procedures. At a minimum, privacy policies and procedures should include:

- Clear roles and responsibilities of key privacy personnel including the Chief Privacy Officer
- Privacy specific knowledge and training requirements for key personnel involved in administering the Department privacy program.

Recommendation 2: We recommend that the United States Capitol Police finalize draft documents related to identifying personally identifiable information that is collected or handled. Additionally, the Department should immediately conduct a review to identify where personally identifiable information is being collected, maintained, processed, or disseminated within the organization. This review should result in an inventory of the types, location, format (hard copy vs. electronic), and the accountable officials related to the personally identifiable information captured.

Recommendation 3: We recommend that the United States Capitol Police finalize draft privacy training materials and require all employees and contractors to periodically complete privacy training (at least annually). In addition, management should track attendance of privacy training to ensure all individuals complete training in accordance with its established policy.

DEPARTMENT COMMENTS

Appendix B
Page 1 of 2



UNITED STATES CAPITOL POLICE

UNITED STATES CAPITOL POLICE
4001 STREET, N.E.
WASHINGTON, DC 20510-7340

March 27, 2009

COP 090320

MEMORANDUM

TO: Mr. Carl W. Hoecker
Inspector General

FROM: Phillip D. Morse, Sr.
Chief of Police

SUBJECT: Response to Draft Report Audit of USCP Privacy Program (Report No. OIG-2009-03).

The purpose of this memorandum is to provide the United States Capitol Police Department's responses to the Office of the Inspector General's (OIG's) *Draft Report Audit of USCP Privacy Program* (Report No. OIG-2009-03).

After review of the audit findings and recommendations, the Department generally concurs with the recommendations in the draft report.

Recommendation 1: We recommend that the United States Capitol Police finalize and fully implement a privacy program. The program should clarify the Chief Privacy Officer's role and the position within the Department as well as include privacy policies and procedures. At a minimum, privacy policies and procedures should include:

- Clear roles and responsibilities of key privacy personnel including the Chief Privacy Officer
- Privacy specific knowledge and training requirements for key personnel involved in administering the Department privacy program.

USCP Response: We generally agree and will clarify the roles and responsibilities of the Chief Privacy Officer, as well as the specific knowledge and training requirements for key privacy personnel in our privacy policies and procedures.

Recommendation 2: We recommend that the Department finalize draft documents related to identifying personally identifiable information that is collected or handled. Additionally, the Department should immediately conduct a review to identify where personally identifiable information is being collected, maintained, processed, or disseminated within the organization. This review

should result in an inventory of the types, location, format (hard copy vs. electronic), and the accountable officials related to the personally identifiable information captured.

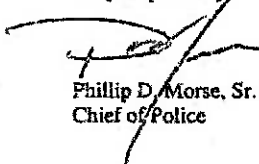
USCP Response: We generally agree and the draft documents will be finalized as soon as possible by the Department's Privacy Board. In addition, the Department is purchasing software that will electronically scan its servers, databases, records or documents to identify those containing personally identifiable information. Upon completion of this e-inventory, the Department will conduct a survey to complete the inventory of its paper documents or records and identify the accountable officials responsible for maintaining these records.

Recommendation 3: *We recommend that the United States Capitol Police finalize draft privacy training materials and require all employees and contractors to periodically complete privacy training (at least annually). In addition, management should track attendance of privacy training to ensure all individuals complete training in accordance with its established policy.*

USCP Response: We generally agree and the draft privacy training materials will be finalized after they are approved by the Department's Privacy Board. Department employees' attendance at privacy training will be recorded in the Department's Training Tracker System. Contractors will be required to sign a training certification sheet which will be tracked and maintained by their respective contractor representatives. All identified Department officials, employees and contractors handling personally identifiable information will sign an acknowledgement form annually to certify their compliance with the Department's policies on handling personally identifiable information and sensitive health information.

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,



Phillip D. Morse, Sr.
Chief of Police

cc: Capitol Police Board
Chief Administrative Officer
Assistant Chief of Police
USCP Audit Liaison

