Privacy Office

Second Quarter Fiscal Year 2010 Report to Congress

Department of Homeland Security Report of the Chief Privacy Officer Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007

March 26, 2010

Homeland Security

Foreword

I am pleased to present the following report, "Privacy Office Second Quarter Fiscal Year 2010 Report to Congress." The *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53, requires the Department of Homeland Security (DHS) Privacy Office to report quarterly regarding: (1) the number and types of review of Department actions undertaken; (2) the type of advice provided and the response given to such advice; (3) the number and nature of complaints received by DHS for alleged violations; and (4) a summary of the disposition of such complaints. In accordance with this requirement, this report serves as the Privacy Office's second quarter report, covering the period from December 1, 2009 to February 28, 2010.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Joseph R. Biden
President, United States Senate

The Honorable Christopher S. Bond
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Susan M. Collins
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Conyers, Jr.
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Peter Hoekstra
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Darrell Issa
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Peter T. King
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Joseph I. Lieberman
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives

The Honorable Silvestre Reyes
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Lamar Smith
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Jeff Sessions
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Bennie G. Thompson
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Edolphus Towns
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

Inquiries relating to this report may be directed to the DHS Privacy Office at 202-235-0780.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

Executive Summary

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, established additional privacy and civil liberties reporting requirements for DHS. Pursuant to the requirements of Section 803, the Privacy Office is providing its second quarter report for fiscal year 2010.

This report covers the privacy complaints and privacy training for the period of December 1, 2009 to February 28, 2010. The Privacy Office works with each of the components of the Department to provide privacy training and expedite processing of complaints from the public.

The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

TABLE OF CONTENTS

INTRODUCTION

The Department of Homeland Security (DHS) Chief Privacy Officer is the first statutorily-mandated Chief Privacy Officer in the federal government. The DHS Privacy Office is founded upon the responsibilities set forth in Section 222 of the Homeland Security Act of 2002 ("Homeland Security Act") [Public Law 107-296; 6 U.S.C. §142], as amended. The mission of the Privacy Office is to sustain privacy protections and to promote transparency of government operations while achieving the mission of the Department. Within the Department, the Chief Privacy Officer implements Section 222 of the Homeland Security Act,[1] the Privacy Act of 1974,[2] the Freedom of Information Act,[3] the E-Government Act of 2002,[4] and the numerous laws, executive orders, court decisions and DHS policies that protect the collection, use, and disclosure of personally identifiable information collected, used, maintained, or disseminated by DHS.

The *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Public Law 110-53, requires the Privacy Office to report quarterly regarding: (1) the number and types of review of Department actions undertaken; (2) the types of advice provided and the responses given to such advice; (3) the number and nature of complaints received by DHS for alleged violations; and (4) a summary of the dispositions of such complaints.[5] In accordance with this requirement, this report serves as the Privacy Office's second quarter report of Fiscal Year (FY) 2010, covering the period from December 1, 2009 to February 28, 2010.[6] The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, established additional privacy and civil liberties reporting requirements for DHS. The Department continues to review a wide variety of activities and procedures within the Department to find opportunities to enhance protections of privacy and civil liberties of individuals.

REVIEWS

The DHS Privacy Office performs a number of different reviews of IT systems and programs that may have a privacy impact. For purposes of Section 803 Reporting, reviews include the following activities:

1. Privacy Threshold Analyses (PTAs) – The DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary through the Privacy Impact Assessment process;
2. Privacy Impact Assessments (PIAs) required under both the E-Government Act of 2002 and the Homeland Security Act of 2002, as amended;
3. Systems of Records Notice (SORNs) and associated Privacy Act Exemptions;
4. Privacy Act Statements as required under Section (e)(3) of the Privacy Act, which provide notice to individuals at the point of collection;

[1] 6 U.S.C. § 101 *et seq.*
[2] 5 U.S.C. § 552a *et seq.*, as amended.
[3] 5 U.S.C. § 552.
[4] 44 U.S.C. § 3501.
[5] *See* 42 U.S.C. § 2000ee-1(f)(1).
[6] The reporting period matches the existing reporting period required for Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) IT Security and Privacy reporting.

5. Computer Matching Agreements;
6. Data Mining Report as defined by Congress under Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007; and
7. Privacy reviews of Information Technology and Program Budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board.

Type of Review	Number of Reviews
Privacy Threshold Analyses	125
Privacy Impact Assessments	17
System of Records Notices and Associated Privacy Act Exemptions	12
Privacy Act (e)(3) Statements	18
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	4
Total Reviews for Q2 FY10	*176*

In addition to the reviews noted in the above table, in preparation for the U.S.-European Union (EU) Joint Review of Passenger Name Records (PNR) held February 8-9 in Washington, DC., the Privacy Office conducted an update to its review of its December 2008 Report Concerning Passenger Name Records derived from flights between the U.S. and the EU 2008. During the review, the Privacy Office found that U.S. Customs and Border Protection (CBP) had taken action to address all six of the outstanding recommendations contained in the 2008 report. In addition, the Privacy Office found that CBP continues to comply with the terms of the 2007 U.S. – EU PNR Agreement. This report can be found at http://www.dhs.gov/privacy under "International Privacy Activities."

At the Department, PIAs represent a substantial effort on the part of Components, Component Privacy Officers, Privacy Points of Contact, and the DHS Privacy Office. The PIA process is one of the key mechanisms used to assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information. As reflected in the Second Quarterly FY 2010 Federal Information Security Management Act (FISMA) Report regarding agency privacy management submitted to the Office of Management and Budget (OMB), 70 percent of the Department's FISMA systems that require a PIA are currently covered by a PIA. A complete list of PIAs conducted during this reporting period can be found at http://www.dhs.gov/privacy. Below are a few examples:

- Haiti Social Media Disaster Monitoring Initiative – The Office of Operations Coordination and Planning, National Operations Center (NOC) launched a 90-day initiative that will conclude in April 2010 to assist DHS and its components involved in the response, recovery, and rebuilding effort resulting from the recent earthquake and after-effects in Haiti. The NOC used this vehicle to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate, assisting with the response, recovery, and rebuilding effort in Haiti. The NOC monitored publicly-available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and to establish a common operating picture.

- 2010 Winter Olympics Social Media Event Monitoring Initiative – The NOC also launched a social media event monitoring initiative that ran for 30 days and concluded on March 10, 2010, to assist the Department and its components involved in the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, British Columbia (BC). The NOC used this vehicle to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate, assisting with the security, safety, and border control associated with the Olympics. The NOC only monitored publicly-available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and to establish a common operating picture. A DHS Privacy Office review of the NOC implementation of this PIA will be covered in the 3rd Quarter Report of the Section 803 reporting requirements.

- Sensor Web – This project is a research and development effort funded by DHS Science and Technology Directorate (S&T) Office of Small Business Innovation Research that seeks to develop and test the effectiveness of a smart sensor system for potential law enforcement and first responder applications. The technologies being tested—video recording technology and analytic tools to interpret and process that video—are technologies that potentially impact the privacy of individuals, both during the tests and in future live settings.

- Academy Information System – The United States Coast Guard Academy (CGA) developed the Academy information system (ACADIS) to provide an information resource for the management of the CGA educational environment including the training and development of all future Coast Guard officers. To support this function, ACADIS processes transactional data for cadet military program records and various facility applications, manages applicant data to facilitate the admissions process, and warehouses data on cadets, prior cadets, faculty, and staff.

During this reporting period DHS published Privacy Act SORNs to support new programs at DHS as well as reviewed, updated, and reissued existing SORNs to reflect system changes and ensure their accuracy. As reflected in the Second Quarterly FY 2010 FISMA Report regarding agency privacy management submitted to OMB, 93 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. Below are a few examples of SORNs that were published during the reporting period and can be found at http://www.dhs.gov/privacy:

- DHS/TSA-023, Workplace Violence Prevention Program System of Records – DHS/TSA developed this SORN to cover records regarding current and former employees and contractors of TSA and members of the public who have been involved in workplace violence at TSA facilities, or while on or because of their official duty, or who are being or have been assisted or counseled by the TSA Workplace Violence Prevention Program. Records include acts, remarks, or gestures that communicate a threat of harm or otherwise cause concern for the safety of any individual at TSA facilities or while on or because of their official duty. These records may include identifying information, information documenting workplace violence, and actions taken by the Workplace Violence Prevention Program or TSA. DHS/TSA has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/TSA will consider individual requests to determine whether or not information may be released.

- DHS/ICE-001, Student Exchange Visitor Information System (SEVIS) of Records – In conjunction with the development and launch of the next generation SEVIS application, called SEVIS II, DHS/ICE modified its system of records notice to propose the collection of additional

information on students, exchange visitors, and their dependents who are in the United States on F, M, or J classes of admission (F/M/J nonimmigrants), and officials of approved schools for and designated sponsors of F/M/J nonimmigrants. Like its predecessor, SEVIS II is an information system that tracks and monitors F/M/J nonimmigrants throughout the duration of their approved participation within the U.S. education system or designated exchange visitor program.

- DHS/ALL-023, Personnel Security Management System of Records – DHS updated and reissued this SORN to include records systems within the Federal Protective Service and records of federal, state, local, and foreign law enforcement personnel who apply for and/or are granted authority to enforce federal laws on behalf of DHS. This SORN is the baseline system for personnel security activities, as led by the DHS Office of the Chief Security Officer, for the Department.

ADVICE AND RESPONSES

During this reporting period, DHS conducted the following privacy training:

- DHS personnel and contractors attended instructor-led privacy training courses in 1,013 instances.
- DHS personnel and contractors took computer-assisted privacy training courses in 22,020 instances.[7]

The **DHS Privacy Office** engaged in the following outreach activities:

Briefings & Publications:

- International Privacy Policy (IPP) Director briefed the DHS Visa Waiver Program (VWP) team on DHS Privacy Office functions, components, and international outreach. The VWP team negotiates agreements with foreign entities which are raising issues of privacy and data protection more frequently.
- Together with the Department of Justice Chief Privacy and Civil Liberties Office the Chief Privacy Officer made a presentation on the U.S. privacy framework to a delegation of Austrian officials on February 1, 2010. The presentation was in support of the Department's efforts to obtain the support of the Government of Austria on the bilateral Preventing and Combating Serious Crimes Agreement.
- The Chief Freedom of Information Act Officer's (FOIA) memorandum to FOIA Officers regarding proactive disclosure and departmental compliance was published to the National Archives and Records Administration, Office of Government Information Services website at http://www.archives.gov/ogis/foia-activities.html on January 4, 2010.
- The Privacy Office released on its public website a white paper on *Cybersecurity and Privacy Protections*, written in coordination with CS&C and NPPD, on February 5, 2010.

Meetings & Events:

The DHS Privacy Office's Federal Advisory Committee Act Committee, the Data Privacy and Integrity Advisory Committee, held its *quarterly* public meeting in Washington, DC on December 3, 2009. The

[7] DHS offers multiple computer training courses. An individual may have taken multiple courses if his or her job requires it.

Chief Privacy Officer updated the Committee on Privacy Office accomplishments since the Committee's last meeting, and provided an update on the Office's new electronic complaint tracking system.

- The Chief Privacy Officer held the quarterly "Privacy Information for Advocates" outreach meeting to update privacy advocates on the activities of the Privacy Office on December 18, 2009.
- The Deputy Chief Privacy Officer traveled to Hong Kong January 4-5, 2010 for the RISE Conference on Ethics and Policy of Biometrics and International Data Sharing. Deputy CPO Kropf gave a presentation on the intersection of privacy and biometrics.
- The Chief Privacy Officer and the TSA Privacy Officer participated in a panel discussion among federal agency Chief Privacy and Civil Liberties Officers at the 15th Annual Meeting of the Privacy Coalition on January 22, 2010.
- The Privacy Office, together with CBP (Office of Field Operations, Office of Intelligence Operations Coordination, and the CBP Privacy Office) and Policy (Office of International Affairs and Screening Coordination Office) hosted a delegation comprised of staff from the European Commission, the United Kingdom Borders Office, German Data Protection Commission, and the Danish Police, for a two-day Joint Review of the Department's use of passenger name records held February 8 and 9, 2010 in Washington, DC.
- The Chief Privacy Officer spoke at the National Fusion Center Conference in New Orleans, LA, first to the Fusion Center Directors, and then as part of a panel (with DHS CRCL) on Privacy & Civil Liberties 101 on February 23 and 24, 2010.
- IPP Director traveled to Hiroshima, Japan for the Asia Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group Meeting held February 24-26, to present to the Data Privacy Subgroup on DHS Implementation of the APEC Privacy Framework as well as the work of the High Level Contact Group Principles completed last November.
- The Director of Privacy Incidents and Inquiries hosted the second Privacy Incident Handling Quarterly Meeting on February 23, 2010. The forum provided an opportunity for the component Privacy Points of Contact and the DHS Enterprise Operations Center managers to share best practices and provide feedback regarding privacy incident management, mitigation, and prevention of privacy incidents.

Press:

- The Chief Privacy Officer was interviewed by *Business Week* regarding the use of social media and identity management services by the federal government and by *CPO Corner*, an online publication of the American Bar Association's E-Privacy Law Committee, for its February 2010 issue.

Component DHS Privacy Offices engaged in the following outreach activities:

FEMA

- Appointed Thomas McQuillan as FEMA's Privacy Officer.
- Published four privacy articles in various FEMA and DHS newsletters.
- Sent an email to FEMA personnel and contractors containing privacy training, resources and contacts.

ICE

- Sent six email messages to all ICE employees featuring privacy protection tips.

NPPD

- Appointed Paula Ferguson of US-VISIT interim Privacy Officer.

TSA

- Sent email messages to TSA workforce to convey information on safeguarding sensitive PII.

- Conducted meetings with the Center for Democracy and Technology on wait time assessment using Bluetooth technology.
- Participated in a speaking engagement at the Privacy Coalition Annual meeting.

USCIS

- Drafted and distributed for internal vetting the USCIS Privacy Incident Response Plan.

US-VISIT

- Presented a privacy overview at the National Defense Industrial Association Biometric Conference.
- Presented a US-VISIT privacy overview to members of the aforementioned February Austrian Delegation from the Federal Chancellor's Office and the Federal Ministry of Interior.

PRIVACY COMPLAINTS AND DISPOSITIONS

For purposes of Section 803 reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with the DHS Privacy Office or DHS Components or programs. The categories of complaints reflected in the table below are aligned with the categories detailed in the Office of Management and Budget's (OMB) Memorandum M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Act and Privacy Management. Complaints are received from U.S. citizens and lawful permanent residents as well as visitors and aliens.[8]

Type of Complaint	Number of Complaints received during this reporting period	Disposition of Complaint		
		Closed-Responsive Action Taken*	In-Progress (Current Period)	In-Progress** (Prior Periods)
Process and Procedure	5	5	0	0
Redress	17	18	0	2
Operational	22	15	8	18
Referred	2	2	0	0
Total	46	39	8	20

*This category may include responsive action taken on a complaint received from a prior reporting period.

**Please note the two redress complaints were inadvertently omitted from the report for Q1and remain under investigation. The 18 operational complaints reported in prior reports remain under investigation due to their complexity and coordination required with other offices. These 20 complaints will be considered closed when the complaints are fully investigated and the appropriate responsive action is taken.

The complaints are separated into four categories:

1. *Process and Procedure.* Issues concerning process and procedure, such as consent, appropriate notice at the time of collection.
   Example: An individual submits a complaint that alleges a program violates privacy by collecting Social Security Numbers without providing proper notice.

[8] *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.*

2. *Redress*. Issues concerning appropriate access, correction of PII, and redress therein.
   Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[9]
3. *Operational*. Issues related to general privacy concerns and concerns not related to transparency or redress.
4. *Referred*. The DHS Component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another federal agency or entity and referred the complaint to the appropriate organization. This category does not include referrals within DHS. The referral category both serves as a category of complaints, and represents responsive action taken by the Department unless they must first be resolved with the external entity.
   Example: An individual has a question about his or her driver's license or Social Security Number, which the DHS Privacy Office refers to the proper agency.

DHS Components and the DHS Privacy Office report disposition of complaints in one of the two following categories by:

1. *Closed-Responsive Action Taken*. The DHS Component or the DHS Privacy Office reviewed the complaint and a responsive action was taken. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.
2. *In-Progress.* The DHS Component or the DHS Privacy Office is reviewing the complaint to determine the appropriate action and/or response. This category identifies in-progress complaints from both the current and prior reporting periods.

Examples of complaints received during this reporting period and their disposition are:

CBP

- An individual sent an email to the CBP Info Center regarding his questioning upon entry to the United States at Chicago O'Hare and CBP's search authority. He expressed his concerns that questions were of a personal nature and too intrusive. He cited the following examples: "What kind of work do you do? Can your income support the family?" The CBP Info center explained CBP's search authority to him and provided him with related Codes of Federal Regulations (CFRs).

TSA

- The TSA Privacy Office received a complaint from an international airline passenger (fine arts student) arriving into the United States complaining that paint and contact lens solution went missing from his luggage as well as damages to a package containing tea. The TSA Privacy Office advised the passenger that his case presented no privacy issue and that airline and airport workers, in addition to TSA personnel, may have access to checked baggage for security purposes. The TSA Privacy Office provided contact information for the TSA Claims Management Branch should the passenger choose to pursue reimbursement for the lost items.

[9] This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report.

CHCO

- An individual reported that she received an unsealed envelope containing her health benefits information via US mail. CHCO Privacy Point of Contact investigated the issue and discovered the office had sent out a batch mailing of health benefits information to DHS employees using a glue stick and the individual's envelope had not remained sealed. The office immediately discontinued the process of mailing health benefits information to employees. The employees are now required to obtain copies of any health benefits documentation through their electronic personnel files.

US-VISIT

- An individual sent a complaint to US-VISIT regarding a biometrics issue. She stated that she had been sent to secondary screening causing her inconvenience at the airport. US-VISIT reviewed her record and discovered that the problem was incorrectly labeled finger prints. Her thumb prints were incorrectly labeled as her index finger prints on the matchers. This caused the prints that were taken on entry to mismatch against the prints on file. US-VISIT corrected her record to the traveler's satisfaction.

- US-VISIT received an email from an individual who wanted to know where to send her I-94 form. For nonimmigrant visitors entering the United States with a visa, there is a requirement to fill a CBP Form I-94. This form has two specific perforated sections to it. The visitor or the carrier representative must complete both sections of CBP Form I-94 upon arrival in the United States. The bottom section of CBP Form I-94 is a departure record and must be returned to U.S. officials upon exiting the United States. This individual had forgotten to turn it in the departure record at the airport and was worried that she would be recorded as an overstay. Since this was not a US-VISIT issue but rather a CBP issue, US-VISIT directed the individual to CBP's webpage with the relevant I-94 information.

CONCLUSION

As required by the 9/11 Act, this second quarter report provides a summary of the Privacy Office's activities from December 1, to February 28, 2010. The Privacy Office will continue to work with Congress, its colleagues in other federal departments and agencies, and the public to ensure privacy is protected in our homeland security efforts.