Privacy Office

Fourth 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

September 30, 2010

Homeland Security

Foreword

I am pleased to present the following report, "Privacy Office Fourth 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 fourth quarter report, covering the period from June 1, 2010 to August 31, 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 703-235-0780.

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 fourth quarter report for fiscal year 2010.

This report covers the privacy complaints and privacy training for the period of June 1, 2010 to August 31, 2010. The Privacy Office works with each of the components of the Department to provide privacy training and expedite the 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 fourth quarter report of Fiscal Year (FY) 2010, covering the period from June 1, 2010 to August 31, 2010.[6] The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

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 information technology (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 the E-Government Act of 2002, the Homeland Security Act of 2002, as amended, by policy or other law;

[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.

3. Systems of Records Notice (SORNs) and associated Privacy Act Exemptions as required under the Privacy Act;
4. Privacy Act Statements as required under Section (e)(3) of the Privacy Act, which provide notice to individuals at the point of collection;
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 IT 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	152
Privacy Impact Assessments	16
System of Records Notices and Associated Privacy Act Exemptions	3
Privacy Act (e)(3) Statements	7
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	91
Total Reviews for Q4 FY10	*269*

PIA

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 sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. As will be reflected in the 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:

- iComplaints – The Office for Civil Rights and Civil Liberties (CRCL) Equal Employment Opportunities (EEO) Program operates the iComplaints Complaint Enterprise System. iComplaints is an electronic records system used to track complaints and supporting documentation relating to individual and class complaints of employment discrimination and retaliation prohibited by DHS civil rights statutes. iComplaints will replace EEO Eagle as EEO Eagle is being decommissioned. CRCL EEO conducted this PIA because iComplaints collects and stores personally identifying information (PII).

- E-Verify Use of Commercial Data for Employer Verification – The Verification Division of the U.S. Citizenship and Immigration Services (USCIS) operates the E-Verify

Program, which provides verification of employment authorization for employers participating in the E-Verify program. The E-Verify Program will collect additional employer business information from both registering employers and a commercial data provider, Dun and Bradstreet, to enhance the employer registration process, manage customer relationships, and improve reporting capabilities and operational effectiveness. This expanded information collection pertains to registered employers participating in the E-Verify Program.

- MyTSA Mobile Application – The Transportation Security Administration's (TSA) MyTSA application consists of a mobile and an iTunes application that provides the traveling public access to relevant TSA travel information via any mobile phone with Internet access. MyTSA enables individuals to access information such as the types of items that may be carried through TSA security checkpoints, basic information regarding TSA checkpoint policies, estimated wait times at TSA checkpoints, and current travel conditions. The MyTSA application does not collect or use PII. This PIA addresses the privacy impact of TSA's use of mobile media for delivering information to the public.

- Watchlist Service – DHS currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the Department of Justice Federal Bureau of Investigation Terrorist Screening Center (TSC) of identifying information about those known or reasonably suspected of being involved in terrorist activity in order to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. DHS and TSC improved the current method of transmitting TSDB data from TSC to DHS. Through a new service called the "DHS Watchlist Service" (WLS), TSC and DHS automated and simplified the current manual process. TSC remains the authoritative source of watchlist data and will provide DHS with near real-time synchronization of the TSDB. DHS will ensure that each DHS component system receives only those TSDB records which they are authorized to use under the WLS Memorandum of Understanding and authorized under existing regulations and privacy compliance documentation between TSC and DHS (WLS MOU) and any amendments or modifications thereto. DHS conducted this PIA because the WLS maintains a synchronized copy of the TSDB, which contains PII, and disseminate it to authorized DHS components.

- Publicly Available Social Media Monitoring and Situational Awareness Initiative – The Office of Operations Coordination (OPS), National Operations Center (NOC) has launched and is leading the Publicly Available Social Media Monitoring and Situational Awareness Initiative (Initiative) to assist DHS and its components involved in fulfilling OPS statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)) to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate. The NOC and participating components may also share this de-identified information with international partners and the private sector where necessary and appropriate for coordination. While this Initiative is not designed to actively collect PII, OPS conducted this PIA because the Initiative could potentially involve PII or other information received in an identifiable form.

SORN

During this reporting period DHS updated, renamed, and reissued one Privacy Act SORN titled, "DHS Office for Civil Rights and Civil Liberties– 001 Matters System of Records," January 6, 2004 to "DHS/ALL-029 Civil Rights and Civil Liberties Records" to capture the expansion of the overall system of records to include both the Department Office for Civil Rights and Civil Liberties, as well as all component offices that perform civil rights and civil liberties functions, and staff components who do not have a designated civil rights and civil liberties office but who do perform related civil rights and civil liberties functions. As reflected in the Fourth Quarterly FY 2010 FISMA Report regarding agency privacy management submitted to OMB, 94 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. All DHS SORNs can be found at http://www.dhs.gov/privacy.

IT Reviews

The Privacy Office reviewed and scored 91 major IT investments through the Office of Management and Budget (OMB) FY 2012 budget submission process to ensure proper privacy documentation. Of the 91 systems reviewed, the Privacy Office failed 11 systems because they lacked privacy compliance documentation. Budget programs that fail for lack of privacy compliance documentation receive higher level scrutiny by component and DHS leadership. The Privacy Office is actively working with the component privacy officers and the program managers to complete the necessary documentation to bring these IT systems into compliance by the next budget review cycle.

Privacy Compliance Review

In addition to the reviews reported in the table on page 2, during this quarter, the Privacy Office published the results of its Privacy Compliance Review (PCR) of the Haiti Social Media Disaster Monitoring Initiative and 2010 Winter Olympics Social Media Event Monitoring Initiative. The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of PCR. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation including PIAs, SORNs and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements.

OPS, including the NOC, launched the Social Networking/Media Capability (SNMC) to assist DHS and its components involved in the response, recovery, and rebuilding effort resulting from the earthquake and after-effects in Haiti as well as the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, British Columbia. In compliance with its statutory obligation, OPS, through SNMC Analysts in the NOC, monitored publicly available online forums, blogs, public websites, and message boards to provide situational awareness and establish a common operating picture. The DHS Privacy Office conducted a PCR of SNMC Analyst activities, as outlined in both the Haiti Social Media Disaster Monitoring Initiative PIA (January 21, 2010) and 2010 Winter Olympics Social Media Event Monitoring Initiative PIA (February 10, 2010). At the time of the PCR, the DHS Privacy Office found that SNMC activities substantially complied with the stated privacy parameters set forth in the underlying

PIAs. However, OPS/NOC had not yet finalized a records retention schedule for SNMC Analyst-generated data including, but not limited to, New Media Monitoring Capability Reports. Since there may be PII in SNMC Analyst-generated data and reports, clearly defining how long that data will be retained is key to minimizing the impact to privacy. Subsequent to the PCR, OPS/NOC has finalized a records retention schedule. The DHS Privacy Office will re-evaluate the records retention schedule as well as conduct a more in-depth review of websites and the applicable social media Internet-based platforms and information technology infrastructure that have been monitored by OPS/NOC as part of the SNMC during the scheduled November 2010 follow-up PCR. The PCR is available at http://www.dhs.gov/privacy.

ADVICE AND RESPONSES

DHS Privacy Training

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

- **3,704** DHS personnel attended instructor-led privacy training courses (note: this metric captures each time a person attends training.)
- **52,926** DHS personnel and contractors completed the mandatory computer-assisted privacy training course: *Culture of Privacy Awareness* (note: this is an annual requirement).

For the **annual period** September 1, 2009 – August 31, 2010, **174,993** DHS personnel and contractors completed the mandatory computer-assisted privacy training course: *Culture of Privacy Awareness.* This equates to 92% percent of the total DHS workforce of 189,000 (total staff as of July 3, 2010, not including contractors).

New Employee Training:

1. The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Component Privacy Offices may also offer introductory privacy training for new employees.
2. The DHS Privacy Office provides privacy training each month as part of the two-day *DHS 101* training course, which is required for all new and existing headquarters staff.

Fusion Center Training:

1. During this reporting period, the DHS Privacy Office continued to collaborate with the Office of Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to staff from many of the Fusion Centers.
2. On June 11, the DHS Privacy Office provided training to intelligence professionals selected for assignment to a Fusion Center from the DHS Office of Intelligence & Analysis, as required under section 511 of the 9/l1 Commission Act.

Compliance Training:

On June 10, the DHS Privacy Office hosted its annual Privacy Compliance Workshop in Washington, D.C. This public workshop was attended by over 100 representatives from DHS, the federal privacy community, and the public.

The Office of the Chief Information Officer (OCIO), Enterprise Business Management Office (EBMO), Paperwork Reduction Act (PRA) Program Management Office (PMO) continues to provide comprehensive PRA training through workshops to the Department's components. This training includes a 30-45 minute presentation by the Privacy Compliance Group on the relationship between privacy and PRA, reduction of PII (particularly Social Security numbers and dates of birth) on information collection request forms, and Privacy Act e(3) Statements. A general privacy overview, including privacy compliance documentation, is also provided. During this reporting period, the Privacy Compliance Group provided training at five PRA workshops.

On August 31, the Privacy Office conducted a Privacy Compliance Boot Camp training that was tailored to component privacy offices. The training covered privacy requirements, an in-depth discussion of the PTA, accountability mechanisms in place for ensuring privacy compliance, and the respective roles and responsibilities of the DHS Privacy Office and component privacy offices. The recently named NPPD Privacy Officer, NPPD staff, new DHS Privacy Office Staff, and USCIS Privacy Office staff attended this training.

DHS Privacy Office Awareness and Outreach Activities

Staff Awareness:

- On August 2, the DHS Privacy Office distributed a new factsheet *How to Safeguard Personally Identifiable Information* about best practices for safeguarding PII to all DHS staff. The factsheet was distributed Department-wide via email and made available on the DHS intranet. Hard copies are now provided to incoming headquarters employees and to many components' incoming employees.
- DHS Privacy Office Speaker Series:
    - On July 15, Joanne McNabb, DHS Data Privacy and Integrity Advisory Committee member and Chief, California Office of Privacy Protection, traveled to Washington, D.C., to discuss privacy protections in California.
    - On July 28, John Shea, Director, Enterprise Services & Integration Office of the Department of Defense's Chief Information Officer, spoke in Washington, D.C., on cloud computing.

Publications:

- In June, the DHS Privacy Office published *The DHS Privacy Office Guide to Implementing Privacy* to provide guidance to federal personnel seeking to establish or streamline a privacy office. A copy is posted on the DHS Privacy Office website.
- Also in June, the DHS Privacy Office undertook a comprehensive review of its privacy compliance guidance and templates aimed at improving the quality and consistency of privacy compliance documentation for the Department. During this process, the Compliance Group sought advice and input from privacy experts including individual members of the Data Privacy and Integrity Advisory Committee (DPIAC), academia, component chiefs of staff, component privacy officers, and PPOCs. Updates reflect more mature compliance processes, increased focus on privacy analysis, and guidance within the templates to aid document preparers in meeting the Compliance Group's high standard. These updates were

rolled out on June 10, 2010 during the DHS Privacy Office's annual privacy compliance workshop.

Meetings & Events:

- Privacy Information for Advocates – On June 4, the Chief Privacy Officer hosted a quarterly Privacy Information for Advocates meeting. The CRCL Officer and the TSA Privacy Officer participated in a discussion about Advanced Imaging Technology.
- Passenger Name Records Outreach. On June 7-11, the Chief Privacy Officer and the Director of International Privacy Policy traveled to Poland, the Czech Republic, and Hungary to advance the DHS position regarding the 2007 U.S. – European Union (EU) Passenger Name Records (PNR) Agreement.
- Government Technology Research Alliance (GTRA) Council Meeting – On June 6, the Associate Director of Privacy Policy and Education was a panelist in a session entitled "How to Create Privacy in a Culture Moving Toward Increased Access of Personal Data" at the GTRA Council Meeting in Bedford, PA.
- State Department International Visitor Program – On June 16, the DHS Privacy Office hosted five visitors from Germany, Austria, Ireland, and the Slovak Republic as part of the State Department's International Visitor Leadership Program.
- Privacy Coalition Outreach Meeting – On July 30, the Chief Privacy Officer addressed the Privacy Coalition, a group of 43 advocacy groups led by the Electronic Privacy Information Center, on privacy and cybersecurity at the Department.
- Social Security Administration Conference – On July 27, the Chief Privacy Officer participated on a privacy panel at the Social Security Administration conference entitled, "Got Data? Get Answers! Understanding Privacy, Disclosure, Freedom of Information and Data Exchange."

Press:

- On June 21, the Chief Privacy Officer and the DHS Assistant Secretary in the Office of Policy participated in a meeting with 12 European journalists at the Foreign Press Center, as part of the Department's outreach to European audiences on the U.S. privacy framework. The meeting resulted in several reports in the press.
- Chief Information Officers Council Article – On July 27, this Council published an article based on an interview with the Chief Privacy Officer about two new publications that offer guidance to federal personnel seeking to establish or streamline a privacy office: *Best Practices: Elements of a Federal Privacy Program*, by the Federal CIO Council Privacy Committee, and the *Guide to Implementing Privacy*, by the DHS Privacy Office.

DHS Component Privacy Office Awareness and Outreach Activities

FEMA

- FEMA began delivering in-person privacy training to its 10 regional field offices. During this reporting period, training was delivered to three regional offices.

ICE

- Four privacy *Tip of the Week* broadcasts were emailed to all ICE Employees.
- The ICE Privacy Office began delivering its *ICE Privacy 101: Everyday Applications* privacy training to program offices located at ICE Headquarters and in the Dallas field office. During this reporting period, 8 training sessions were delivered to a total of 216 ICE employees.
- The ICE Privacy Office conducted 10 in-person privacy training sessions for 31 program office points of contact regarding the use and posting of sensitive PII on ICE SharePoint collaboration sites.
- ICE Privacy Officer presented and demonstrated the Online Detainee Locator System during a press conference.
- ICE Privacy Officer gave a presentation to seven Non-Governmental Organizations (NGOs) about privacy at ICE and addressed concerns about detainee privacy.
- ICE Privacy Officer presented and discussed the ICE Privacy Waiver Form for disclosing information (including PII) to third parties with various NGOs.

TSA

- TSA Privacy Officer released the fourth edition in the "Privacy Man" poster series designed to raise staff awareness of the importance of safeguarding personally identifiable information.
- TSA Privacy Officer attended the Computers, Freedom, and Privacy Conference in San Jose, CA and provided a briefing titled: *Privacy and Security at the Federal, State, and Local Levels*.

US VISIT

- For one week in August, US-VISIT Today (a daily US-VISIT online newsletter) ran a privacy message entitled "The Importance of Safeguarding Personally Identifiable Information" to raise employee awareness of data protection and privacy. The message linked to the new DHS Privacy Office factsheet, *How to Safeguard Personally Identifiable Information*.

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.[7]

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	6	6	0	0
Redress	6	6	0	2
Operational	61	55	11	2
Referred	8	8	0	0
Total	81	75	11	4

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

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.
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.[8]
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

[7] *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*.
[8] This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report.

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

With increased presence of Border Patrol checkpoints on the Northern Border, the CBP INFO Center has seen an increase in the number of complaints regarding privacy and CBP's search authority. CBP has taken proactive steps to make information available regarding Border Patrol checkpoints and the CBP inspection process by posting information on http://www.cbp.gov/,[9] producing an informational brochure for the public explaining the enforcement purpose of the checkpoints, and a coordinated effort with the CBP INFO Center and the Office of Border Patrol to provide information to the public and address their concerns.

- In June, a U.S. Citizen contacted the CBP INFO Center requesting information on a Border Patrol checkpoint in New Hampshire. He inquired as to the legality of the checkpoints and asked what authority permits Border Patrol Agents to request identification from U.S. Citizens and question them about their travel plans. A response was provided to the individual citing the various laws under the United States Code that CBP enforces, as well as providing 19 C.F.R. 162.6, from which border search is derived. After clarifying that CBP has jurisdiction within 100 miles of the border, the complainant was satisfied with the response.

[9]See http://www.cbp.gov/xp/cgov/border_security/border_patrol/border_patrol_ohs/overview.xml, http://www.cbp.gov/xp/cgov/border_security/border_patrol/, https://help.cbp.gov/app/answers/detail/a_id/1022/kw/checkpoint, and http://www.cbp.gov/linkhandler/cgov/border_security/border_patrol/border_patrol_ohs/national_bp_strategy.ctt/national_bp_strategy.pdf.

- A U.S. Citizen from Vermont contacted the CBP INFO Center requesting information on the Border Patrol's search authority and jurisdiction. A verbal explanation was provided and a follow-up email was sent providing the individual with CBP's search authority, an overview of Border Patrol checkpoints, and per his request links to additional information for research purposes. The individual was satisfied with the information provided.

TSA

- The TSA Office of Privacy Policy and Compliance responded to a traveler's complaint and inquiry into whether TSA Transportation Security Officers violated his Health Insurance Portability and Accountability Act (HIPAA) rights by screening his Continuous Positive Airway Pressure (CPAP) machine in public. CPAP Machines are used primarily in the treatment of sleep apnea. TSA responded to the individual by acknowledging that TSA recognizes that screening procedures can be more difficult for persons with medical conditions and that it is difficult to prevent other passengers from seeing medical devices exposed at the security checkpoint. TSA also advised the traveler that TSA is not a "covered entity" under HIPAA. In addition, TSA provided the individual a link to information from TSA's website for travelers with special needs and identified a specific link directed to CPAP screening.

US-VISIT

- US-VISIT received a redress request from an individual who informed US-VISIT that his family had encountered difficulties during their last visit to the United States. At the airport, his two daughters' biographics and biometrics were interchanged so that each daughter's prints were associated with the biographics of the other, causing mismatched records. US-VISIT researched the issue and discovered the individual was correct. US-VISIT took corrective action to amend the records of both of the daughters so that the incorrect encounters were deleted, thus ensuring an improved travel experience in the future.

CONCLUSION

As required by the 9/11 Act, this fourth quarter report provides a summary of the Privacy Office's activities from June 1, 2010 to August 31, 2010. The Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure privacy is protected in our homeland security efforts.