Privacy Office

Third 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

June 23, 2010

Homeland Security

Foreword

I am pleased to present the following report, "Privacy Office Third 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 third quarter report, covering the period from March 1, 2010 to May 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 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 third quarter report for fiscal year 2010.

This report covers the privacy complaints and privacy training for the period of March 1, 2010 to May 31, 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 third quarter report of Fiscal Year (FY) 2010, covering the period from March 1, 2010 to May 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 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.
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;

[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.

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	172
Privacy Impact Assessments	16
System of Records Notices and Associated Privacy Act Exemptions	8
Privacy Act (e)(3) Statements	3
Computer Matching Agreements	2
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews for Q3 FY10	*201*

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 reflected in the Third Quarter 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:

- BP Oil Spill Response Social Media Event Monitoring Initiative - The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), launched an April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative to assist DHS and its components involved in the security, safety, and emergency response associated with the BP oil spill response off the Gulf Coast. The NOC is using 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 emergency response associated with the oil spill. The NOC is only monitoring 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. OPS will not set up user accounts to access any information. While this Initiative is not designed to collect personally identifiable information (PII), OPS conducted a PIA because the Initiative could receive PII or other information received in an identifiable form.

- Integrated Common Analytical Viewer (Sensitive but Unclassified) – DHS/National Protection and Programs Directorate implemented the Integrated Common Analytical Viewer (iCAV SBU), a sensitive but unclassified, secure, web-based, geospatial visualization tool that integrates commercial and government-owned data and imagery from multiple sources enabling homeland security partners to establish comprehensive situational and strategic awareness across the nation and around the globe to better prepare for, prevent, respond to and recover from natural and man-

made disasters. DHS/NPPD conducted a PIA to analyze and evaluate any privacy impact resulting from the use of visualization technology.

- Malware Lab Network - The Malware Lab Network (MLN) contributes critical support to existing tools used by the US Computer Emergency Readiness Team (US-CERT) to advance the risk-reduction segment of the Department's overall mission. Specifically, the US-CERT provides key capabilities in four cyber mission areas: 1) Alert, Warning, and Analysis; 2) Coordination and Collaboration; 3) Response and Assistance; and 4) Protection and Detection. The MLN collects, uses, and maintains analytically relevant information in order to support the Department's cyber security mission, including the prevention and mitigation of cyber attacks, protection of information infrastructure, the assessment of cyber vulnerabilities, and response to cyber incidents. DHS is conducted this PIA to publicly analyze and evaluate PII within the MLN.

- E-Verify Program - DHS published two PIAs related to the E-Verify Program. The Verification Division of USCIS provides a service that allows employers to verify the employment eligibility of their newly-hired employees through an electronic verification program called E-Verify. Previously, USCIS addressed the E-Verify program as part of the Verification Information System PIA. USCIS conducted a separate PIA for E-Verify in order to better assist the public in understanding this program overall. Further, USCIS conducted a PIA update to the E-Verify PIA to provide additional transparency into its use of commercial data for employer registration. Specifically this PIA update provides transparency into the expanded information collection on registered employers participating in the E-Verify Program. The PIA update describes the additional employer business information from both registering employers and a commercial data provider, Dun and Bradstreet (D&B), to be collected in order to enhance the employer registration process, manage customer relationships, and improve reporting capabilities and operational effectiveness.

- Data Analysis & Research for Trade Transparency System – DHS/ICE operates the Data Analysis and Research for Trade Transparency System (DARTTS), which supports ICE investigations of trade-based money laundering, contraband smuggling, and trade fraud. DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. These anomalies are then independently confirmed and further investigated by experienced ICE investigators. The PIA for DARTTS was first published in October 2008. ICE is migrating DARTTS to the ICE Enterprise Network, and has added two new sets of financial data and a new set of trade data. ICE also implemented new audit features and capabilities to enhance integrity and accountability. ICE updated and republished the DARTTS PIA to reflect these changes.

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 Third 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/CISOMB-001, Virtual Ombudsman System of Records – DHS developed this SORN to cover records associated with processing of information to aid the Citizenship and Immigration Services Ombudsman in providing assistance to individuals, employers, and their representatives in resolving problems with USCIS; identify areas in which individuals, employers, and their representatives have problems working with U.S. Citizenship and Immigration Services; and to

the extent possible, propose changes to mitigate problems pursuant to 6 U.S.C. § 272.

- DHS/USCIS-011, E-Verify Program System of Records - DHS/USCIS developed this SORN to cover records associated with the E-Verify Program (as part of the program-wide approach to the E-Verify Program PIA discussed earlier). The U.S. Citizenship and Immigration Services E-Verify Program allows employers to check citizenship status and verify employment eligibility of newly hired employees. Previously, these records were covered under DHS/USCIS--004 Verification Information System of Records, December 11, 2008, along with records from the U.S. Citizenship and Immigration Services Systematic Alien Verification for Entitlements (SAVE) Program. In order to provide clearer transparency and enable public understanding, the Department separated out records from the Verification Information System of Records into two separate systems of records for the E-Verify and SAVE Programs.

- TSA Biennial Review – During this reporting period, DHS/TSA reviewed and republished five DHS/TSA SORNs as part of the Department's in accordance with OMB requirements to biennially review, and republish, if necessary, Departmental SORNs. The five SORNs updated and reissued as part of the biennial review included:

    - DHS/TSA-001, Transportation Security Enforcement Record System, DHS/TSA-001(covers records related to the TSA's screening of passengers and property and enforcement actions involving all modes of transportation regulated by the TSA);
    - DHS/TSA-002, Transportation Security Threat Assessment System (covers records related to security threat assessments, employment investigations, and evaluations TSA conducts on certain individuals for security purposes);
    - TSA-006, Correspondence and Matters Tracking Records (covers records associated with the management, tracking, retrieval, and response to incoming correspondence, all outgoing correspondence, memoranda, documentation, injuries, claims, and complaints associated with all subject matters over which TSA exercises jurisdiction);
    - TSA-011, Transportation Security Intelligence Service Operations Files (covers records on individuals identified in intelligence, counterintelligence, transportation security and information systems security records that relate to TSA's mission); and
    - TSA-013, Federal Flight Deck Officer Record System (covers records necessary for assessment, acceptance, training, participation, and recertification of deputized pilots of commercial air carriers who participate in the Flight Deck Officer Program designed to defend aircraft flight decks against acts of criminal violence or air piracy).

ADVICE AND RESPONSES

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

- DHS personnel and contractors attended instructor-led privacy training courses in ***3,402*** instances.

- 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. A new 30-minute course was rolled out in April 2010.
    2. During the past year, the DHS Privacy Office provided a privacy presentation each month as part of the two-day *DHS 101* training course, which is now required for all new and existing headquarters staff. The content for this course was also revised and re-launched in March 2010.

- Fusion Center Training: During this reporting period, the Director of Legislative and Regulatory Analysis and the Associate Director of Training collaborated with the Office of Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to newly appointed privacy officers from each of the Fusion Centers.

- DHS personnel and contractors completed computer-assisted privacy training courses in ***47,554*** instances.[7]

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

Websites:

- The DHS Privacy Office launched a greatly improved public website (http://www.dhs.gov/privacy) to increase public usability and transparency of Privacy Office activities in April 2010. The enhanced website features new navigation, a new home page with an intuitive roadmap making it easier to locate privacy and FOIA information, as well as improved content throughout the site.

Meetings & Events:

- Data Privacy and Integrity Advisory Committee (DPIAC): The DPIAC held public meetings in Washington, DC on March 18 and May 25, 2010. The latest meeting included remarks by the Secretary of Homeland Security, who thanked the Committee for its advice on various DHS programs and emphasized the importance of protecting core American values, including privacy, as the Department works to secure the country from the terrorist threat.
- Privacy Information for Advocates: The Chief Privacy Officer hosted a quarterly outreach meeting to update privacy advocates on the activities of the Privacy Office on March 26, 2010.
- Chief Privacy Officer Support for Transatlantic Information Sharing and Privacy: The Chief Privacy Officer traveled to Brussels, Strasbourg, Amsterdam, The Hague, and Berlin on March 6-12, in an effort to urge support for the U.S.-European Union Passenger Name Record Agreement that is subject to a ratification vote before the European Parliament. The Chief Privacy Officer met with Members of the European Parliament, key officials at ministries of justice and interior, and engaged in public outreach.
- OECD Working Party for Information Security and Privacy Roundtable: The International Privacy Policy (IPP) Director joined an inter-governmental delegation representing the U.S. at the Organization for Economic Development and Cooperation (OECD) Working Party for Information Security and Privacy and a Privacy Roundtable March 8-10, on the impact of the OECD Privacy Guidelines.

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

- Privacy Office Speaker Series: The Privacy Office Speaker Series hosted Daniel J. Weitzner, Associate Administrator for Policy, National Telecommunications & Information Administration of the Department of Commerce on March 22, for a discussion of the nexus between internet policy and innovation.
- International Association of Privacy Professionals: The Deputy Chief Privacy Officer moderated and presented a panel on international information sharing agreements on April 20.
- DHS Privacy Exchange Program: The Privacy Office hosted four officials: two from the Canadian Ministry of Justice, one from the Spanish Ministry of the Interior and one from the Spanish Ministry of Justice as well as the liaison from the German Ministry of Interior April 19 – 22. This is part of an ongoing exchange program to provide outreach to our foreign partners about DHS' privacy framework. In addition to meeting with representatives from the Privacy Office, participants met with other DHS components, as well as other U.S. government agencies with privacy and data protection responsibilities.
- Privacy as a Foreign Policy: The Chief Privacy Officer spoke at the State Department's annual Deputy Chiefs of Mission (DCM) Conference, which brought in nearly 70 DCMs from the European and Eurasian Affairs Bureau and the International Organizations Affairs Bureau on May 19. The Chief Privacy Officer led a discussion on "Cultural Divide? Data Privacy and Security" with 16 DCMs.
- Information Sharing Environment Outreach: The Chief Privacy Officer spoke at the Information Sharing Environment Privacy and Civil Liberties Advocacy Group Roundtable regarding the privacy requirements for fusion centers on May 20.

Press:

- U.S.-EU Passenger Name Records: During March, the Chief Privacy Officer was covered in numerous European press regarding privacy issues surrounding the U.S. – EU Passenger Name Record agreement and other DHS programs.

Component DHS Privacy Offices engaged in the following privacy outreach activities:

USCIS

- The Second Annual Verification Division Privacy Awareness Month was held in May 2010 as a vehicle to train employees on privacy policies and best practices. The Chief Privacy Officer was the keynote speaker at the event kick-off.

FEMA

- The FEMA Privacy Office presented at the FEMA Individual Assistance ESF #6 Conference held in San Diego, CA from April 27 through 30, 2010. The FEMA Deputy Privacy Officer and FEMA Individual Assistance staff spoke on the topic "Privacy Act – Discussion of New Routine Uses and the Process for Information Sharing."

ICE

- The ICE Privacy Officer briefed the staff of the House Homeland Security Committee on May 5, 2010.
- The ICE Privacy Officer participated in a panel discussion on May 17, 2010 as part of the USCIS National Immigration Conference, briefing 250 Congressional staffers on privacy disclosure requirements to Congress.
- The ICE Privacy Officer spoke at the Data Privacy and Integrity Advisory Committee meeting on May 25, 2010.
- The ICE Privacy Office sent three email messages to all ICE employees featuring privacy protection tips.

SCIENCE & TECHNOLOGY

- The S&T Privacy Office held its third annual privacy awareness training event in April 2010 (Privacy Week 2010). Activities included mandatory privacy awareness training for all S&T employees and contractors, including personnel at S&T offsite laboratories. The Chief Privacy Officer was a keynote speaker at the April S&T All Hands Meeting to kick off this event.

TSA

- The TSA Privacy Office sent one email message to all TSA employees featuring privacy protection tips.
- The TSA Privacy Office provided a privacy overview to 70 participants at the United States Department of Agriculture Privacy Conference.

US COAST GUARD

- To increase privacy awareness throughout the component, USCG sent two representatives to the annual Information System Security Managers Conference in Orlando, Florida the week of April 12, where they presented a privacy overview to 150 participants.

US-VISIT

- On April 21, 2010, US-VISIT Privacy Officer participated in a panel session titled, "Effective Privacy Lifecycle Management in U.S. Government Agencies" at the International Association of Privacy Professionals (IAPP) Global Privacy Summit held in Washington D.C. He discussed US-VISIT's privacy program and the processes in place to prevent and react to privacy incidents.

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	2	2	0	2
Operational	31	50	6	1
Referred	15	15	0	0
Total	53	72	6	3

*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.[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:

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

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

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

The CBP INFO Center has received numerous complaints and inquiries from travelers regarding the collection and retention of PII. Several complaints concerned the collection of fingerprints and photographs of travelers. Two examples are provided below.

- In May, an Italian traveler questioned the collection of his fingerprints and photograph at JFK airport, and inquired as to how this information would be used and shared. He also commented that the collection of this information made him feel as if he was a criminal. His e-mail was responded to with an explanation for collecting biographical data, the CBP inspection process, and a link was provided to the US-VISIT website. The traveler was satisfied with CBP's response.

- A traveler at the Dallas Fort-Worth airport questioned "what does the CBP and the government do with the information that was entered into the system about me and what impact will it have on me in the future both in my travels personally/professionally (i.e. background checks, etc.)?" CBP responded to the traveler's e-mail with information regarding the collection of passenger name records (PNR) and biographical data citing relevant privacy policies for both collection. The traveler was satisfied with the response.

CBP has taken proactive steps to make information regarding the receipt and use of PNR data, US-VISIT data collection, and the CBP inspection process by posting privacy policies, frequently asked questions, links to appropriate government websites, and fact sheets, to the public CBP web site, www.cbp.gov. This information can also be obtained by contacting the call center and tear sheets provided to interested travelers at the ports of entry.

TSA

- The TSA Office of Privacy Policy and Compliance responded to a number of complaints objecting to full-body scans by Advanced Imaging Technology (AIT), such as the "Backscatter" or "Millimeter Wave" technologies. Specifically, TSA responded to these complaints by outlining the strong privacy protections in place for use of AIT which are also documented in related PIAs. These protections include: the image operator never sees the passenger; the image generated by the technology is not sufficient to identify the passenger; and TSA does not retain the image. In addition, passengers have the option to decline the technology in favor of a physical pat-down. This choice is prominently explained on signs placed in airport queues prior to arriving at the technology. Reliance on signage over a verbal explanation by a Transportation Security Officer to every passenger ensures that passengers are made aware of their choices, and that the message is consistent.

US-VISIT

- G-4 visa holders are exempt from US-VISIT procedures and are not required to submit their biometrics upon arrival at a port of entry in the United States. A G-4 visa is a type of nonimmigrant U.S. visa for employees of international organizations and members of their immediate families. US-VISIT received a redress letter by mail from a G-4 visa holder who had been erroneously fingerprinted. He requested that his fingerprints be deleted from the US-VISIT system. US-VISIT checked his records and discovered that his fingerprints had already been deleted from the system. No further action to correct his record at US-VISIT was required at the time. US-VISIT sent a letter to the individual indicating his biometrics had been deleted from the US-VISIT system.

CONCLUSION

As required by the 9/11 Act, this third quarter report provides a summary of the Privacy Office's activities from March 1, 2010 to May 31, 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.