Department of Homeland Security

Privacy Office

Second Quarter Fiscal Year 2012 Report to Congress

May 31, 2012

Homeland Security

I. FOREWORD

May 31, 2012

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Second Quarter Fiscal Year 2012 Report to Congress*. This quarterly report includes activities from December 1, 2011 – February 29, 2012.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] (*9/11 Commission Act*) requires the DHS Privacy Office to report quarterly on the:

- Number and types of privacy reviews of Department actions undertaken;
- Type of advice provided and the response given to such advice; and
- Number and nature of privacy complaints received by DHS for alleged violations along with a summary of the disposition of such complaints.

In addition, we include information and data on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

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

The 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") as amended.[3] The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act,[4] the *Privacy Act of 1974*,[5] the *Freedom of Information Act*[6] (FOIA), the *E-Government Act of 2002*,[7] and the numerous laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of personally identifiable information (PII) by DHS.

---

[1] The reporting period for this report matches the required reporting period under *The Federal Information Security Management Act of 2002* ("FISMA", 44 U.S.C. § 3541, *et seq.*) rather than the fiscal year.
[2] 42 U.S.C. §2000ee-1(f)
[3] 6 U.S.C. §142
[4] 6 U.S.C. §142
[5] 5 U.S.C. §552a
[6] 5 U.S.C. §552
[7] Pub. L. 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. §101 note.]

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

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

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

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

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

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

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

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

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

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

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

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

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

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C. A. Dutch Ruppersberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Inquiries about this report may be directed to the DHS Privacy Office at 703-235-0780 or privacy@dhs.gov. This report and other information about the Office are available on our website, listed below.

Sincerely,

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

DHS PRIVACY OFFICE
SECOND QUARTER FISCAL YEAR 2012
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act*, 42 U.S.C. § 2000ee-1, includes the following requirement:

> (f) Periodic Reports-
>
> (1) IN GENERAL- The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than quarterly, submit a report on the activities of such officers--
>
> (A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;
>
> (ii) to the head of such department, agency, or element; and
>
> (iii) to the Privacy and Civil Liberties Oversight Board; and
>
> (B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.
>
> (2) CONTENTS- Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including--
>
> (A) information on the number and types of reviews undertaken;
>
> (B) the type of advice provided and the response given to such advice;
>
> (C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and
>
> (D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

III. PRIVACY REVIEWS

The DHS Privacy Office reviews programs and information technology (IT) systems that may have a privacy impact. During this reporting period, the DHS Privacy Office is adding a category to this report to highlight its conduct of Privacy Compliance Reviews.

For purposes of this report, reviews include the following DHS Privacy Office activities:

1. Privacy Threshold Analyses (PTA), 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 (PIA) required under the *E-Government Act of 2002* and the *Homeland Security Act of 2002*, as amended, and by DHS policy;
3. Systems of Records Notices (SORN) 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* to provide notice to individuals at the point of collection;
5. Computer Matching Agreements as required under the *Privacy Act*;
6. Data Mining Report as required by Section 804 of the *9/11 Commission Act;* [8]
7. Privacy Compliance Reviews; and
8. Privacy reviews of IT and program budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board.

[8] 42 U.S.C. §2000ee-3

Reviews Conducted During Second Quarter Fiscal Year 2012	
Review Type	**# of Reviews**
Privacy Threshold Analyses	178
Privacy Impact Assessments	13
System of Records Notices and Associated *Privacy Act* Exemptions	1
Privacy Act (e)(3) Statements	1
Computer Matching Agreements	5
Data Mining Reports	1
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews	***201***

A. Privacy Impact Assessments

The Privacy Impact Assessment process is one of the key mechanisms used to assure that the Department's programs and technologies sustain, and do not erode, privacy protections for DHS' use, collection, and disclosure of PII. As of February 29, 2012, 80 percent of the Department's Federal Information Security Management Act (FISMA) systems requiring a PIA were subject to a PIA. This represents a slight decrease from the 81 percent reported subject to a PIA during the prior period due to additional systems coming online. Additionally, the Department has implemented a triennial review program for existing PIAs to assess and confirm that the systems covered under those PIAs are still operating within the originally published parameters. As these triennial reviews are completed, previously-published PIAs will be updated to inform the public that a review has been completed for the affected systems.

The Department published 13 PIAs during this reporting period and seven of them are summarized below. PIAs conducted by DHS can be found on our website, www.dhs.gov/privacy. *Please note that any update to an existing PIA is listed with a small letter after the number for the original PIA.*

DHS/USSS/PIA-007 Forensic Services Division (FSD) Polygraph System

Background: The FSD Polygraph Branch of the United States Secret Service (USSS) uses the FSD Polygraph System to track all polygraph examinations that USSS administers. This database contains information on applicant and criminal suspect polygraph examinations and their results.

Purpose: USSS conducted this PIA because the system contains the PII of individuals who undergo polygraph exams. *(December 15, 2011)*

DHS/ALL/PIA-028(a) Freedom of Information Act (FOIA) and Privacy Act (PA) Records Program Update

Background: The DHS Privacy Office updated the PIA describing the use of PII in DHS FOIA and PA processes and systems.

Purpose: This update describes the use of a new FOIA software application for tracking FOIA requests. *(December 16, 2011)*

DHS/FEMA/PIA-020 Integrated Financial Management Information System (IFMIS) Merger

Background: FEMA's Office of the Chief Financial Officer operates the IFMIS-Merger system, FEMA's official accounting and financial management system. IFMIS-Merger pulls financial data from other FEMA, DHS, and government-wide systems (subsystems), and is the source of data for both internal and external financial reporting. The system also records and tracks financial transactions.

Purpose: FEMA conducted this PIA because IFMIS-Merger collects, uses, maintains, retrieves, and disseminates PII pulled from the subsystems. *(December 16, 2011)*

DHS/USSS/PIA-008 Secret Service Use of Advanced Imaging Technology (AIT)

Background: USSS has deployed AIT at Secret Service protective sites. AIT is used as a secondary means of personnel screening at protected sites, and is only used after the primary screening measures indicate that an individual requires an additional level of screening. This technology creates an image of the body and highlights any anomalies that may appear on the body.

Purpose: The USSS conducted this PIA to address its potential collection of PII through the use of AIT. It was determined that PII is not collected from individuals who are identified for secondary screening using this technology. The image of the individual is not linked in any way to PII, and the AIT does not have the capability to store, transmit, or print these images. *(December 23, 2011)*

DHS/ALL/PIA-041 One DHS Overstay Vetting Pilot

Background: DHS is conducting the One DHS Overstay Vetting Pilot to improve DHS' ability to identify and vet foreign nationals who have remained in the United States beyond their authorized period of admission (overstays). The pilot will streamline data sharing between the National Protection and Programs Directorate's United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE). The overstay vetting process is covered by existing PIAs for the CBP Automated Targeting System, US-VISIT Technical Reconciliation Analysis Classification System, and US-VISIT Arrival and Departure Information System. Data sharing conducted through this program allows DHS to better identify which individuals have overstayed their authorized periods of admission, and, of those overstays, which are the highest law enforcement or national security priority for enforcement action by ICE.

Purpose: DHS conducted this PIA to increase transparency for the increased sharing of PII about travelers within DHS that this pilot requires. *(December 29, 2011)*

DHS/TSA/PIA-036 Transportation Safety Administration (TSA) Canine Website System (CWS)

Background: Under the Aviation and Transportation Security Act, the TSA is responsible for security in all modes of transportation. TSA's National Explosives Detection Canine Team Program (NEDCTP) prepares dogs and handlers to quickly locate and identify dangerous materials that may present a threat to transportation systems. The NEDCTP operates the CWS, which is a web-based system designed to assist in coordinating operations. The CWS is the central management database for all NEDCTP records and operations.

Purpose: TSA conducted this PIA for CWS because it collects PII about members of the public in an identifiable form in order to facilitate training, foster communication, and perform administrative functions. *(January 13, 2012)*

B. Systems of Record Notices

As of February 29, 2012, 96 percent of the Department's FISMA systems that require a SORN were covered by an applicable SORN. SORNs receive biennial reviews to ensure that they conform to and comply with the standards outlined in the *Privacy Act*. If no update is required, the SORN remains intact.

All DHS SORNs and Final Rules for Privacy Act Exemptions can be found on our website, www.dhs.gov/privacy.

During this reporting period, DHS published one Final Rule for Privacy Act Exemptions:

DHS/FEMA-012 Suspicious Activity Reporting System of Records Notice Final Rule

DHS issued a final rule to amend its regulations to exempt a newly established system of records titled, "DHS/Federal Emergency Management Agency-012 Suspicious Activity Reporting System of Records" from certain provisions of the *Privacy Act*. Specifically, the Department exempts portions of the "DHS/Federal Emergency Management Agency-012 Suspicious Activity Reporting System of Records" from one or more provisions of the *Privacy Act* to meet criminal, civil, and administrative enforcement requirements. *(January 10, 2012)*

C. Privacy Compliance Reviews

The DHS Privacy Office uses Privacy Compliance Reviews (PCRs) to assure that DHS programs and technologies implement and maintain appropriate privacy protections for PII. 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 Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements.

During this reporting period, the DHS Privacy Office conducted and published the results of two PCRs. Reports on the results of PCRs can be found on our website www.dhs.gov/privacy.

ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service

The U.S. Government Accountability Office (GAO) recently reviewed selected DHS systems that support counterterrorism, including the U.S. Immigration and Customs Enforcement Pattern Analysis and Information Collection System (ICEPIC) Law Enforcement Sharing (LEIS) Service. GAO's review concluded that the LEIS Service was not described adequately in the January 2008 ICEPIC PIA. GAO recommended that the Chief Privacy Officer investigate whether the LEIS component of ICEPIC should be deactivated until an updated PIA describing the LEIS component was approved. DHS concurred with the recommendation, and, as a result of the reports' findings and recommendations, the DHS Privacy Office initiated this PCR. The review revealed that the ICEPIC PIA required an update which was completed and published on October 26, 2011.
(December 15, 2011)

EINSTEIN Program

The DHS National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD) launched the EINSTEIN program in 2004. EINSTEN is a computer network intrusion detection system that helps protect federal executive agency information technology enterprises. NCSD conducted, and the DHS Privacy Office reviewed and approved, PIAs for each phase of the EINSTEIN program. As NCSD made plans for the next phase of the program, EINSTEIN 3, the DHS Privacy Office conducted a PCR to ensure the accuracy of compliance documentation, and the transparency of the EINSTEIN program as it moves forward.
(*January 3, 2012*)

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

34,005 DHS personnel completed the mandatory computer-assisted privacy training course, Culture of Privacy Awareness. This course must be taken by all new personnel and annually thereafter.

New Employee Training

1,295 DHS personnel attended instructor-led privacy training courses, primarily privacy training for new employees:

- The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees.
- The DHS Privacy Office provides privacy training each month as part of the two-day *DHS 101* course, which is required for all new and existing headquarters staff.
- Many of the Component Privacy Officers[9] also offer introductory privacy training for new employees.

Fusion Center Training

- The DHS Privacy Office collaborates with the Office of Intelligence and Analysis (I&A) and the Office for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to staff at state and major urban area fusion centers.
    - *During this reporting period, **42** people were trained in **2** sessions at **2** fusion centers.*
- The DHS Privacy Office provides training to I&A intelligence professionals selected for assignment to fusion centers, as required under section 511 of the *9/11 Commission Act*.
    - *During this reporting period, **one** new analyst was trained on privacy policy.*

Nationwide Suspicious Activity Reporting Initiative

- The DHS Privacy Office also provides training to Suspicious Activity Reporting (SAR) analysts.
    - *During this reporting period, **31** SAR analysts were trained on privacy issues related to suspicious activity reporting.*

[9] Each of the 10 sub-Components that comprise the Department has a Privacy Officer.

B. DHS Privacy Office Awareness & Outreach

Publications

Privacy Incident Handling Guidance (PIHG) – In January 2012, the Privacy Office issued a revised version of the PIHG, which provides detailed guidance for all stages of privacy incident handling, including reporting, escalation, investigation, mitigation, notification, and closure.

The PIHG can be found on the DHS Privacy Office website: www.dhs.gov/privacy

Outreach

The DHS Privacy Office sponsored an outreach event open to all federal workers during this reporting period:

- *DHS Privacy Office Speaker Series* – On January 11, 2012, in Washington, D.C., DHS provided an overview of the operational cybersecurity program and system known as EINSTEIN/NCPS, and the planned strategy for future cybersecurity protections across the Federal Government.

Meetings & Events

- Privacy at the National Defense University (NDU) – On December 6, 2011, the Deputy Chief Privacy Officer co-presented to a class at NDU on the federal privacy framework.
- Data Privacy and Integrity Advisory Committee (DPIAC) – On December 6, 2011, the DPIAC held a public meeting in Washington, DC. Following the Chief Privacy Officer's update, the Privacy Officer of the DHS Office of Intelligence and Analysis gave an overview of his office's implementation of DHS privacy policy. The Committee also voted on two draft reports that proposed recommendations on building privacy protections (from both policy and technology perspectives) into the intra-departmental information sharing infrastructure.
- Privacy Information for Advocates Meeting – On December 9, 2011, the Chief Privacy Officer hosted a quarterly meeting designed to proactively engage the privacy community on current privacy issues. The meeting covered a variety of topics, including the department's use of social media to support its various missions.
- Chief Privacy Officer (CPO) Presentation at Inaugural International Privacy Policy Training Session – On January 12, 2012, the Chief Privacy Officer, along with officials from the Departments of State, Justice and Commerce and the Federal Trade Commission, provided an overview on privacy and foreign policy to a class of approximately 25 Foreign Service Officers. This was the first in a proposed series of privacy trainings for Department of State's diplomatic corps.

C. Component Privacy Office Awareness & Outreach

National Protection and Programs Directorate (NPPD) Office of Privacy

The NPPD Office of Privacy engaged in the following activities this quarter:

- Provided specialized privacy training to two Federal Protective Service (FPS) groups in Philadelphia, PA. The first training session, held at the Philadelphia MegaCenter, focused on privacy and law enforcement. The second session was delivered to the FPS Acquisitions staff and focused on implementing privacy in the acquisitions process. This session was the first step in a larger effort to ensure Federal Government contractors comply with DHS privacy training and incident handling requirements.
- Provided specialized privacy training to two groups within the Office of Infrastructure Protection. For the Infrastructure Security Compliance Division, the NPPD Office of Privacy provided training on the privacy compliance process and development of compliance documentation. For the Sector Outreach and Programs Division, the NPPD Office of Privacy provided training designed to help the division identify activities that may trigger privacy requirements.
- Continued its efforts to provide specialized training to all human capital personnel, providing two separate briefings to the Professional Development & Training and Workforce Analysis branches.
- Participated in a two-day training session hosted by the Information Management Division at which NPPD briefed FPS regional Freedom of Information Act (FOIA) processors on the intersection between the FOIA and the Privacy Act. The training included privacy-related best practices for FOIA professionals.
- Hosted a Lunch & Learn event entitled *Smartphone Privacy, Who's Tracking and Who's Hacking You?*, featuring the Privacy Officer of the DHS Office of Science and Technology.
- Published its second *Privacy Update*, a quarterly publication aimed at increasing overall awareness of privacy within the NPPD community.
- Rolled out a new *E-mail Best Practices Guide*, aimed at educating employees as to effective e-mail practices that help minimize the impact to personal privacy and avoid privacy incidents.

U.S. Immigration & Customs Enforcement Privacy Office

- ICE Privacy Officer delivered a presentation on Sensitive PII to the Office of the Principal Legal Advisor Chief Counsel's meeting on December 7, 2011, in Washington, D.C.

V. 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 following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Complaints are received from U.S. citizens, Legal Permanent Residents, visitors, and aliens.[10]

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 & Procedure	6	6	2	1
Redress	4	5	0	1
Operational	236	249	15	13
Referred	2	3	0	0
Total	***248***	***263***	***17***	***15***

*This category may include responsive action taken on a complaint received from a prior reporting period.
**This category reflects an additional complaint that was not accounted for in a prior reporting period.

Complaints are separated into four categories:

1. ***Process and Procedure:*** Issues concerning process and procedure, such as consent, or 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 and/or correction of PII, and appropriate redress of such issues.
   Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[11]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
   Example: An employee's health information was disclosed to a non-supervisor.
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 a complaint must first be resolved with the external entity.

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

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:

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.

The following are examples of complaints received during this reporting period, along with disposition:

U.S. Customs and Border Protection

Complaint:
The CBP INFO Center received a verbal complaint from a U.S. citizen who is studying in The Hashemite Kingdom of Jordan. The complainant noted that she experienced delays in boarding her flight to the U.S., and was escorted off the airplane when she arrived at JFK airport. She stated that she "felt humiliated and like a criminal" when her laptop, personal papers, and other documents were searched. She further complained that she was "interrogated without just cause" and that the questions asked regarding her Jordanian husband were "unnecessary."

Disposition:
This complaint was referred to the Office of the Port Director, who responded to the complainant with a formal letter explaining CBP's border search authority for inspecting electronic devices. This letter further identified the types of questions she was asked as being within CBP's authority.[12] The traveler was also offered the opportunity to go through the DHS Traveler Redress Inquiry Program.

[12] CBP's border search authority of electronic devices emanates from multiple sections of Titles 8 and 19 of the U.S.C., as well as §401 in Title 22 and §5317 in Title 31.

Transportation Security Administration

Complaint:
The TSA Privacy Office received a complaint from an employee stating that a co-worker had heard information about a Letter of Reprimand the complainant received merely five minutes prior. The co-worker informed the complainant that another employee was the source of the information.

Disposition:
The TSA Privacy Office contacted the complainant and learned the individuals who shared the information about the Letter of Reprimand were managers at the airport where the employee worked. The TSA Privacy Office contacted the Federal Security Director (FSD) responsible for the managers and advised the FSD to admonish the managers involved and to counsel them on the importance of limiting *Privacy Act* information to individuals with a need to know the information in the performance of their duties. The TSA Privacy Office also participated in a nationwide teleconference with all FSDs to emphasize the importance of limiting access to *Privacy Act* protected information, and the potential harm from unauthorized disclosure of such information.

U.S. Visitor and Immigrant Status Indicator Technology

Complaint:
US-VISIT received an inquiry from a married couple who encountered difficulties during their entry into the United States.

Disposition:
US-VISIT reviewed their records in IDENT and determined that the wife's fingerprints were found to be of poor quality, thus creating individual Fingerprint Identification Numbers (FINs) for two of her entries. Additionally, one record had her husband's biometrics attached to her biographics. US-VISIT corrected the mismatch and consolidated the wife's two FINs into a single FIN.

VI. CONCLUSION

As required by the *9/11 Act*, this second quarter 2012 report provides a summary of the DHS Privacy Office's activities from December 1, 2011 – February 29, 2012. The DHS Privacy Office will continue to work with Congress, colleagues in other Federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.