Department of Homeland Security

Privacy Office

Second Quarter Fiscal Year 2013 Report to Congress

May 2013

Homeland Security

I. FOREWORD

May 31, 2013

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Second Quarter Fiscal Year 2013 Report to Congress* for the period December 1, 2012 – February 28, 2013.[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 following activities:

- 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 Chief Privacy Officer is the first statutorily-mandated Chief Privacy Officer in the Federal Government. Section 222 of the *Homeland Security Act of 2002* (Homeland Security Act),[3] sets forth the responsibilities of the DHS Privacy Office. 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, the *Privacy Act of 1974*[4] (Privacy Act), the *Freedom of Information Act*[5] (FOIA), and the *E-Government Act of 2002*[6] (E-Government Act), along with numerous other laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of personally identifiable information by DHS.

[1] The reporting period for this report corresponds with the period established for reporting under *The Federal Information Security Management Act of 2002* (FISMA, 44 U.S.C. § 3541) rather than the October through September fiscal year.
[2] 42 U.S.C. § 2000ee-1(f).
[3] 6 U.S.C. § 142.
[4] 5 U.S.C. § 552a.
[5] 5 U.S.C. § 552.
[6] 44 U.S.C. § 101 note.

Pursuant to Congressional notification requirements, the DHS Privacy Office is providing this report to the following Members of Congress:

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn, M.D.
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 Michael McCaul
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 Bob Goodlatte
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

Please direct any inquiries about this report to the DHS Privacy Office at 202-343-1717 or privacy@dhs.gov. This report and other information about the Office are available on our website, www.dhs.gov/privacy.

Sincerely,

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security

DHS PRIVACY OFFICE
SECOND QUARTER FISCAL YEAR 2013
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, sets forth the following requirements:

"(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.

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), as required under the E-Government Act, the Homeland Security Act,[7] and DHS policy;

3. System of Records Notices (SORN), as required under the Privacy Act[8] and any associated Final Rules for Privacy Act exemptions;[9]

4. Privacy Act Statements, as required under the Privacy Act[10] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[11]

6. Data Mining Reports, as required by Section 804 of the 9/11 Commission Act; [12]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the Homeland Security Act;[13]

8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board; and

9. Other privacy reviews, such as implementation reviews for information sharing agreements.

[7] 6 U.S.C. § 142.
[8] 5 U.S.C. § 552a(e)(4).
[9] 5 U.S.C. § 552a(j), (k).
[10] 5 U.S.C. § 552a(e)(3).
[11] 5 U.S.C. § 552a(o)-(u).
[12] 42 U.S.C. § 2000ee-3.
[13] 6 U.S.C. § 142.

Table I: Reviews Completed Second Quarter Fiscal Year 2013	
Type of Review	**Number of Reviews**
Privacy Threshold Analyses	142
Privacy Impact Assessments	20
System of Records Notices and Associated Privacy Act Exemptions	7
Privacy Act (e)(3) Statements	19
Computer Matching Agreements	1
Data Mining Reports	1
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests	0
Other Privacy Reviews	5
Total Reviews	***195***

A. Privacy Impact Assessments

The Privacy Impact Assessment process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections for the use, collection, and disclosure of personally identifiable information (PII). As of February 28, 2013, 86 percent of the Department's Federal Information Security Management Act (FISMA) systems requiring a PIA had one in effect.

In addition to completing PIAs for systems not currently subject to a PIA, the Department conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the originally published parameters. After the Department completes a triennial review, it updates any previously published PIAs to inform the public that it has completed a review of the affected systems.

During the reporting period, DHS published 20 new, updated, or renewed PIAs, and seven are summarized below. Published PIAs are available on our website, www.dhs.gov/privacy.

Updates to existing PIAs appear with a lower-case letter in parentheses after the original PIA number.

DHS/ALL/PIA-002 – DHS Traveler Redress Inquiry Program (TRIP) Three-Year PIA Review (*Originally published January 2007)*
Background: The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) is a web-based customer service initiative developed as a voluntary program to provide a one-stop mechanism to request redress for individuals who believe they have been: (1) denied or delayed boarding transportation due to DHS screening programs; (2) denied or delayed entry into or departure from the United States at a port of entry; or (3) identified for additional (secondary) screening or inspection at transportation facilities, including airports and seaports. DHS TRIP provides traveler redress intake and processing support and works with DHS components to review and respond to requests for redress.

Purpose: DHS completed a three-year review of the DHS TRIP PIA to document any changes to its privacy risks, and found that there were no changes that required a PIA update. The PIA will be reviewed in another three years or if system changes occur.

DHS/NPPD/USVISIT/PIA-002 – Automated Biometric Identification System (IDENT) *(December 7, 2012)*
Background: IDENT is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses.

Purpose: This PIA provides transparency on how the system uses PII and describes the system's sharing partners and functions.

DHS/USSS/PIA-011 – Cyber Awareness Program (Cyveillance) *(December 14, 2012)*
Background: The U.S. Secret Service uses the Cyveillance system as part of its Cyber Awareness Program. Cyveillance searches for information regarding the Secret Service and investigatory and protective intelligence information.

Purpose: The Secret Service conducted this PIA because, while the primary purpose of Cyveillance is not to collect PII, the content collected by Cyveillance may contain PII.

DHS/S&T/PIA-008 – Standoff Technology Integration and Demonstration Program Update *(December 19, 2012)*
Background: The DHS Science and Technology Directorate (S&T), Resilient Systems Division, is using the Standoff Detection Test Bed to test and evaluate the Biometric Optical Surveillance System (BOSS). BOSS is a facial recognition technology that matches 3D signatures from captured facial images with enrolled images stored in the system database.

Purpose: S&T conducted this PIA to address privacy concerns raised by testing the facial recognition technology.

DHS/CBP/PIA-002 – Global Enrollment System (GES) *(January 10, 2013)*
Background: The Global Enrollment System allows U.S. Customs and Border Protection (CBP) to handle the enrollment and vetting processes for the trusted traveler and registered traveler programs in a centralized environment. Individuals who wish to apply to participate in these programs voluntarily provide PII to CBP in return for facilitated clearance at designated U.S. border ports of entry (POE) upon acceptance.

Purpose: CBP conducted this PIA to describe its trusted traveler programs, including specific improvements to the Global Entry trusted traveler program and to the Global Online Enrollment System, which is the standard application process for almost all CBP trusted traveler programs. This PIA also describes CBP's registered traveler programs, which include the Small Vessel Reporting System and the Decal and Transponder Online Procurement System. The GES PIAs dated April 20, 2006, and November 1, 2006, were retired upon publication of this PIA.

DHS/NPPD/PIA-028 – Enhanced Cybersecurity Services (ECS) *(January 16, 2013)*
Background: ECS is a voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating Commercial Service Providers. The purpose of the program is to assist the owners and operators of critical infrastructure in enhancing the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. ECS consists of the operational processes and security oversight required to share unclassified and classified cyber threat indicators with companies that provide internet, network, and communication services to enable those companies to enhance their services to protect U.S. Critical Infrastructure entities. ECS is intended to support U.S. Critical Infrastructure; however, pending deployment of EINSTEIN[14] intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating federal civilian Executive Branch agencies.

Purpose: The National Protection and Programs Directorate conducted this PIA because PII may be collected. This PIA consolidates and serves as a replacement to the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA, published on January 13, 2012, and the DHS/NPPD/PIA-021(a) National Cyber Security Division Joint Cybersecurity Services Program

[14] Privacy Impact Assessments for DHS cybersecurity programs, including EINSTEIN, can be found at: http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

(JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS) PIA Update, published on July 18, 2012.

DHS/CBP/PIA-013 – Customs-Trade Partnership Against Terrorism (C-TPAT) *(February 14, 2013)*
Background: C-TPAT is a CBP voluntary trade partnership program between CBP and private businesses to build relationships that strengthen international supply chains and improve U.S. border security, in which CBP and members of the trade community work together to secure and facilitate the movement of legitimate international trade. The program focuses on improving security throughout the supply chain, beginning at the point of origin (including manufacturer, supplier, or vendor) through the point of distribution to the destination. C-TPAT member companies, called partners, implement certain security procedures throughout their supply chains and in return receive facilitated processing by CBP,improving security while facilitating the flow of global trade.

Purpose: In the course of enrolling, certifying, and validating C-TPAT applicants/partners and their supply chains, the C-TPAT system will receive PII and confidential business information from the applicant/partner, as well as sensitive law enforcement information from existing law enforcement systems.

B. System of Records Notices

As of February 28, 2013, 97 percent of the Department's FISMA systems that require a System of Records Notice (SORN) had 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 original SORN remains in effect.

During the reporting period, DHS published five SORNs and two Notices of Proposed Rulemaking, and two are summarized below. All DHS SORNs, Notices of Proposed Rulemaking and Final Rules for Privacy Act exemptions are available on our website, www.dhs.gov/privacy.

DHS/CBP-002 - Global Enrollment System
CBP updated and reissued a current DHS system of records titled, "DHS/CBP-002 Global Enrollment System (GES)." Global Entry (GE) is a CBP program that enables CBP to facilitate the inspection and security process of lower risk, pre-approved travelers, and allows more scrutiny for those travelers who present an unknown risk. GE, previously a pilot program, is now a permanent trusted traveler program (77 Fed. Reg. 5681, Feb. 6, 2012). CBP re-published this system of records notice to update the categories of records, authorities, purposes, routine uses, retrievability, retention and disposal, notification procedures, record sources, and Privacy Act exemptions for this system of records.

- ***DHS/CBP-002 - Global Enrollment System, Notice of Proposed Rulemaking for Privacy Act Exemptions***
  Concurrently with the GES SORN, DHS published a Notice of Proposed Rulemaking in which the Department proposed to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (78 Fed. Reg. 4079, January 18, 2013.)

DHS/CBP-004 - Intellectual Property Rights e-Recordation and Search Systems
CBP established a new DHS system of records titled, "DHS/CBP-004-Intellectual Property Rights e-Recordation and Search Systems System of Records (IPRRSS)." The system collects, uses, and maintains records related to intellectual property rights recordations and their owners. IPRRSS aids in the enforcement of intellectual property rights by making intellectual property recordations available to the public and to CBP officials.

- ***DHS/CBP-004 - Intellectual Property Rights e-Recordation and Search Systems, Notice of Proposed Rulemaking for Privacy Act Exemptions***
  Concurrently with the SORN, DHS published a Notice of Proposed Rulemaking in which the Department proposed to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (78 Fed. Reg. 4347, January 22, 2013.)

C. Privacy Compliance Reviews

The DHS Privacy Office uses Privacy Compliance Reviews (PCR) to ensure DHS programs and technologies implement and maintain appropriate privacy protections for PII. Consistent with the DHS Privacy Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

The DHS Privacy Office continued worked on several ongoing PCRs, but did not complete any PCRs during this reporting period.

Reports on the results of PCRs are available on our website, www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

35,904 DHS personnel completed the mandatory computer-assisted privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter.

New Employee Training

2,127 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[15] also offer introductory privacy training for new employees.

Fusion Center Training

- The DHS Privacy Office provides training to Office of Intelligence and Analysis (I&A) intelligence professionals selected for assignment to fusion centers, as required under Section 511 of the *9/11 Commission Act.*[16]
    - *DHS Privacy Office trained three analysts on privacy policy.*

Nationwide Suspicious Activity Reporting Initiative

- The DHS Privacy Office provides training to Suspicious Activity Reporting (SAR) analysts.
    - *DHS Privacy Office trained 57 analysts on privacy issues related to suspicious activity reporting.*

[15] 10 DHS offices and components have a Privacy Officer.
[16] Pub. L. 110-53, §511, 6 U.S.C. §101 note.

B. DHS Privacy Office Awareness & Outreach

Publications

In February 2013, the DHS Privacy Office published the *2012 Data Mining Report to Congress*. This annual report describes DHS programs, both operational and in development, that involve data mining as defined by the *Federal Agency Data Mining Reporting Act of 2007*. The report can be found on our website, www.dhs.gov/privacy.

Meetings & Events

- Privacy Information for Advocates Meeting – On January 16, the Acting Chief Privacy Officer hosted a quarterly meeting to proactively engage the privacy community on current privacy issues.
- American University Washington College of Law's (WCL) Collaboration on Government Secrecy Program – On January 17, the Freedom of Information Act Operations Senior Director participated as a panelist in a program titled "*Transparency in the Obama Administration: A Fourth-Year Assessment*," which discussed the Office of Government Information Services' successful discharge of its statutory mandate, and more, during its first three years.
- Federal Aviation Administration Privacy Week Symposium – On January 29, the Acting Chief Privacy Officer moderated a panel for the Federal Aviation Administration's Privacy Week Symposium entitled, "*Navigating Turbulence: Meeting the Privacy Challenge*," which focused on federal privacy challenges and best practices.
- Privacy and Civil Liberties Oversight Board Overview – On February 14, the Acting Chief Privacy Officer met with the Privacy and Civil Liberties Oversight Board to provide a brief overview of the roles and responsibilities of the DHS Privacy Office.
- U.S.-Canada Immigration Information Sharing Agreement – On February 27, the DHS Privacy Office participated in an interagency meeting between DHS, including I&A, CBP, U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), and the Department of State in preparation for bilateral discussions with Canada regarding implementation of the U.S.-Canada Immigration Information Sharing Agreement. The bilateral discussions occurred in Ottawa on March 19-20, 2013.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency

- Provided training to all new headquarters employees and contractors using new employee and new contractor orientations.
- Delivered specialized privacy awareness training to personnel in the Logistics Management Division and contractor support staff in the Office of Security.

Federal Law Enforcement Training Center

- Hired a new Information Management Officer to serve as the Component Privacy Officer.

National Protection and Programs Directorate

- Provided two privacy briefings to contracting officer representatives supporting the US-VISIT Program and the Offices of Cybersecurity & Communications, respectively, in order to introduce new guidance on core privacy provisions for NPPD solicitations and statements of work.
- Provided refresher training to the contracting officer representatives of the Office of Infrastructure Protection.
- Presented at the Library of Congress' *National Data Privacy Day Seminar* on January 30. The presentation, which drew 60 attendees, was titled "Key Ingredients – Protecting Your Privacy Information" and incorporated the DHS Fair Information Practice Principles (FIPPs) as key ingredients for protecting PII.
- Co-hosted training, in tandem with the DHS Office for Civil Rights and Civil Liberties, on privacy, civil rights, and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products. This is part of a series of training events following NPPD's release of an external product checklist that will help employees evaluate privacy, civil rights, and civil liberties concerns.
- Presented at the quarterly NPPD Executive Secretariat All Hands Meeting to provide guidance on how to incorporate the Fair Information Practice Principles into correspondence and task management.
- Released an edition of *Privacy Update*, NPPD's quarterly privacy awareness publication. This quarter's issue focused on the "Privacy by Design" concept, providing a recap of NPPD's October 2012 Privacy Week event, as well as privacy tips and information on recently published privacy guidance.
- Distributed tips on protecting information about government employees, particularly when providing information to third parties associated with conference registrations or training events, in an effort to raise awareness about the threat of hacking and phishing attacks.
- Provided employees with privacy tips, such as how to protect information on Internet-enabled devices while traveling and accessing public Wi-Fi networks or hot spots.
- Published guidance on protecting information from accidental disclosures, to include advising employees on ways to identify and understand the risks associated with metadata and hidden content in documents, and encouraging employees to follow procedures for clearing such documents of sensitive information before sharing them externally.

Office of Intelligence and Analysis

- Published an article in the quarterly I&A staff newsletter on the importance of safeguarding PII.
- Created a privacy blog on the classified network where the Privacy Officer discusses the Fair Information Practice Principles and their applicability to I&A's mission.

Science and Technology Directorate

- Attended the National Institute of Standard and Technology's *Workshop on Cloud Computing and Big Data* in January 2013.

Transportation Security Administration

- Presented best practices for safeguarding Sensitive PII, along with the role of the TSA Privacy Office, to newly hired legal staff.
- Provided training to 45 project team members on the Privacy Act, along with best practices for safeguarding PII.
- Partnered with TSA Sensitive Security Information (SSI) to distribute materials to over 1,000 SSI coordinators highlighting the types of documents containing SSI vs. Sensitive PII.
- Distributed information to all TSA employees on how to protect files when using networked copiers.
- Reviewed approximately 14 intelligence products for sensitive privacy information.

U.S. Coast Guard

- Attended the Federal Aviation Administration's *National Data Privacy Week Symposium* on January 29.

U.S. Citizenship and Immigration Services

- Partnered with the USCIS Mail Management Branch to visit a United Parcel Services (UPS) location to observe how UPS handles and processes packages/parcels. This visit assisted the USCIS Office of Privacy in making recommendations for updating the Records Operation Handbook on best practices for handling and mailing Sensitive PII to prevent privacy incidents.
- Published the USCIS Office of Privacy first quarter newsletter, which focused on the importance of properly disposing of PII and Sensitive PII when it is no longer needed, in addition to other helpful privacy news, tips and guidance for safeguarding PII.
- Published several Privacy Tips that focused on the appropriate use, access, sharing and disposing of PII.
- Partnered with the USCIS Office of Security and Integrity, USCIS Record Management Branch, and USCIS Office of Chief Counsel to develop and broadcast a video on how to safeguard sensitive but unclassified (SBU) information.
- Partnered with the USCIS Records Management Branch to develop a privacy training that focused on best practices for safeguarding sensitive PII and the USCIS process for reporting privacy incidents.
- Trained the Northeast Region Office of Chief Counsel on the Disclosure of PII to Third Parties and best practices for safeguarding PII.
- Trained the USCIS Research and Evaluations Division on privacy compliance and how to work with the USCIS Office of Privacy on research projects that may involve PII.

- Trained the HQ Field Operations Directorate and SharePoint Enterprise Collaboration Network (ECN) Facilitators on privacy requirements for sharing and storing Sensitive PII on the ECN.
- Trained the HQ Field Operations Directorate and Refugee, Asylum and International Operations on privacy compliance requirements for the USCIS Forms Process.

U.S. Immigration and Customs Enforcement

- 392 ICE employees completed *Privacy Training for SharePoint Collaboration Site Users 2012*.
- ICE Privacy Officer and Privacy Branch staff presented at an ICE Freedom of Information Act Office training on February 20, discussing privacy waivers and other disclosures under the Privacy Act, privacy violations and best practices, and ICE Privacy and Records Office responsibilities.

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*. U.S. citizens, Legal Permanent Residents, visitors, and aliens submit complaints.[17]

Table II: Type and Disposition of Complaints Received in the Reporting Period

Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed, Responsive Action Taken	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	7	7	0	1
Redress	1	1	0	0
Operational	586	659	32	19
Referred	0	0	0	0
Total	***593***	***666***	***32***	***20***

.

DHS separates complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *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.
    a. *Example*: Misidentifications during a credentialing process or during traveler inspection at the border or screening at airports.[18]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *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 internal referrals within DHS. The referral category both serves as a category of complaints and represents

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

[18] This category excludes FOIA 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.

responsive action taken by the Department, unless a complaint must first be resolved with the external entity.

a. *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 took responsive action. 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 their disposition:

Transportation Security Administration (TSA)

Complaint: TSA was contacted by an individual who had received a telephone call from TSA attempting to verify his personal information. The individual did not understand why he was contacted and was concerned that his identity had been stolen.

Disposition: TSA's investigation revealed that a Transportation Worker Identification Credential (TWIC) applicant incorrectly listed a telephone number on the application that matched the telephone number of the complainant. The incorrect telephone number had resulted in a misplaced telephone call. TSA reported this finding to the complainant who was satisfied with the resolution..

U.S. Citizenship and Immigration Services (USCIS)

Complaint: USCIS received a complaint from an USCIS employee regarding an allegation of inappropriate access of the employee's resume by a supervisor. The complainant alleged that the supervisor accessed the resume without a need-to-know; the information was potentially misused; and it was not necessary to review the resume beyond the hiring process.

Disposition: The USCIS Office of Privacy launched an investigation by speaking with the supervisor, and it was determined that the access and use of the information was appropriate. Additionally, the employee was advised to meet with the supervisor to discuss these concerns. The complaint was resolved to the employee's satisfaction.

U.S. Customs and Border Protection (CBP)

Complaint: The CBP INFO Center was contacted by a Canadian citizen because she was denied entry into the United States. The complainant noted that she was denied entry despite providing CBP authorities with her DHS Traveler Redress Inquiry Program (DHS TRIP) redress number and final disposition letter from DHS TRIP, which had been obtained five months earlier.

Disposition: The CBP INFO Center contacted the Office of Field Operations Targeting Center, which reviewed its records and determined that the complainant was clear to travel to the U.S. The complainant was notified that she was now cleared to travel to the U.S.

U.S. Immigration and Customs Enforcement (ICE)

Complaint: An ICE employee submitted a complaint to the ICE Privacy Branch after documents containing Sensitive PII were improperly disclosed by an ICE attorney to an administrative law judge. The employee was concerned about being susceptible to identity theft and/or financial loss if the documents were inappropriately handled, as well as the possible exposure of Sensitive PII should the documents become public record.

Disposition: After determining that the employee's Social Security Number should have been redacted before the documents were submitted to the judge, the ICE Privacy Branch contacted the attorney who inadvertently left the documents unredacted. Upon learning of the oversight, the attorney redacted the documents and filed a motion to have the unredacted documents replaced with the redacted version of the documents. The judge granted this motion. The ICE Privacy Branch responded to the complainant explaining the steps taken to redact the documents, and the protocols in place within the judge's office to ensure Sensitive PII is properly handled and protected, minimizing the risk of identity theft and/or financial loss. Additionally, the Privacy Branch explainedthat the administrative law court docket was closed to the public so the information would not become a matter of public record.

VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from December 1, 2012 – February 28, 2013. 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.