Department of Homeland Security

Privacy Office

Second Quarter Fiscal Year 2014 Report to Congress

June 2014

Homeland Security

Foreword

June 23, 2014

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Second Quarter Fiscal Year 2014 Report to Congress* for the period December 1, 2013 – February 28, 2014.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] 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 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] the *Freedom of Information Act*,[5] and the *E-Government Act of 2002*,[6] along with numerous other 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 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 provides 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. More information about the DHS Privacy Office, along with copies of prior reports, is available on the Web at: www.dhs.gov/privacy.

Sincerely,

Karen Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

DHS PRIVACY OFFICE
SECOND QUARTER FISCAL YEAR 2014
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act of 2007*,[7] 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."

[7] 42 U.S.C. § 2000ee-1.

III. PRIVACY REVIEWS

The Department of Homeland Security (DHS or Department) Privacy Office (DHS Privacy Office or 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, 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, as required under the *E-Government Act of 2002*, the *Homeland Security Act of 2002*,[8] and DHS policy;

3. System of Records Notices, as required under the *Privacy Act of 1974*[9] (Privacy Act), and any associated Final Rules for Privacy Act exemptions;[10]

4. Privacy Act Statements, as required under the Privacy Act[11] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[12]

6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*; [13]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the *Homeland Security Act of 2002*;[14]

8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 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.

[8] 6 U.S.C. § 142.
[9] 5 U.S.C. § 552a(e)(4).
[10] 5 U.S.C. § 552a(j), (k).
[11] 5 U.S.C. § 552a(e)(3).
[12] 5 U.S.C. § 552a(o)-(u).
[13] 42 U.S.C. § 2000ee-3.
[14] 6 U.S.C. § 142.

Table I: Reviews Completed *Second Quarter Fiscal Year 2014*	
Type of Review	**Number of Reviews**
Privacy Threshold Analyses	100
Privacy Impact Assessments	12
System of Records Notices and Associated Privacy Act Exemptions	2
Privacy Act (e)(3) Statements	5
Computer Matching Agreements	0
Data Mining Reports	1
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[15]	0
Other Privacy Reviews	0
Total Reviews	***120***

[15] The Chief Information Office prepares a privacy score once a year as part of its Office of Management and Budget Exhibit 300 reporting. Therefore, reviews for this category are calculated only once a year and are included in the fourth quarter report.

A. Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections. As of February 28, 2014, 91 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 new systems and 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, the Office published 12 new, updated, or renewed PIAs. Since all published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy, we only include a summary of the key PIAs here, along with a hyperlink to the full text.

DHS/USCIS/PIA-040 Center Adjudication System Electronic Process *(February 3, 2014)*
The United States Citizenship and Immigration Services (USCIS) developed the Center Adjudication System Electronic Processing (CasePro) system to assist with the adjudication of Temporary Protected Status (TPS), Deferred Enforced Departure (DED), and Deferred Action for Childhood Arrivals (DACA) filings. CasePro electronically organizes and reviews incoming filings, identifies approvable cases, automates the adjudication of some cases that meet filing requirements, and routes filings requiring additional review to the manual resolution process. USCIS conducted this PIA to describe how CasePro collects, uses, and maintains PII.

DHS/ICE/PIA-003 electronic Travel Document System (*February 6, 2014*)
U.S. Immigration and Customs Enforcement (ICE) owns and operates the electronic Travel Document (eTD) System. eTD provides an efficient means for ICE personnel to request, and foreign consular officials to review and adjudicate travel document requests for aliens who have been ordered removed or granted voluntary departure from the United States but do not possess valid travel documents. The PIA for eTD was originally published on October 13, 2006. Since that time, several technical releases have been made to improve the overall efficiency of the system, and a flag has been added to identify aliens with a criminal record, thus necessitating the updating and re-publication of the PIA.

DHS/CBP/PIA-023 Biographic Visa and Immigration Information Sharing with Canada (*February 10, 2014*)
Under the United States-Canada Biographic Visa and Immigration Information Sharing (BVIIS) program, the Department makes certain biographic information from its systems of records available to the Department of Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency (CBSA) via query through the Department of State's (DOS) Consular Lookout and Support System (CLASS). CIC and CBSA will use the information to assist in the administration and enforcement of Canada's immigration laws. Similarly, CIC and CBSA will make certain biographic information from the Global Case Management System (GCMS), the system Canada uses to process applications for citizenship and immigration services, available to DHS via query through CLASS. DHS will use this information to assist in the administration and enforcement of the United States' immigration laws. This PIA provides notice to the public regarding the information sharing and resulting privacy impacts of the BVIIS program.

DHS/CBP/PIA-006(c) Automated Targeting System – TSA/CBP Common Operating Picture (*January 31, 2014*)

The Automated Targeting System (ATS) is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. The PIA was last updated June 1, 2012. This update evaluates the privacy impacts of the Common Operating Picture program, which permits the Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) to share certain information about watchlisted travelers and their traveling companions, as a new part of ATS.

B. System of Records Notices

As of February 28, 2014, 98 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 the DHS Privacy Office published one SORN update and one Final Rule for Privacy Act Exemptions. These documents are summarized below, and a hyperlink to the *Federal Register Notice* is included. All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available on the DHS Privacy Office website, www.dhs.gov/privacy.

DHS/TSA-001 Transportation Security Enforcement Record System (*December 9, 2013*)
This system of records notice allows the TSA to collect and maintain records related to its screening of passengers and property, as well as records related to the investigation or enforcement of transportation security laws, regulations, directives, or federal, state, local, or international law. For example, records related to an investigation of a security incident that occurred during the screening of a passenger or property would be covered by this system. As a result of a biennial review of this SORN, the routine uses were updated. Specifically, the statute citation in routine use [P] has been corrected. This notice was re-issued in its entirety in order to have a single updated SORN available for public review.

DHS/TSA-021 Transportation Security Administration Pre✓™ Final Rule (*January 2, 2014*)
The Department of Homeland Security issued a final rule to amend its regulations to exempt portions of a newly established system of records titled, Department of Homeland Security/Transportation Security Administration-021, TSA Pre✓™ Application Program System of Records, from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

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 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 and Memoranda of Agreement.

During the reporting period, the Office initiated two PCRs which are ongoing:

1. DHS initiated a PCR of CBP's Analytical Framework for Intelligence (AFI), as required by the June 2012 Privacy Impact Assessment. AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border.

2. DHS initiated a sixth PCR on the Office of Operations Coordination and Planning National Operations Center's (OPS/NOC) Publicly Available Media Monitoring and Situational Awareness Initiative, and will issue a publicly available report on the results of the review next quarter.

PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review. Public PCR reports are available on the DHS Privacy Office 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 Online Training

51,131 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.

Classroom Training

1,674 DHS personnel attended instructor-led privacy training courses, including the following:

- **New Employee Training:** The DHS Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees.
    - Many of the Component Privacy Officers[16] also offer privacy training for new employees when they onboard.
    - The DHS Privacy Office provides monthly privacy training as part of the two-day course, *DHS 101*, which is required for all new and existing headquarters staff.

- **DHS 201 International Attaché Training:** The Department's "DHS 201" training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The DHS Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies. The Office trained 26 participants in two training sessions during the reporting period.

- **DHS Security Specialist Course**: The Office provides privacy training each month to participants of the week-long training program. During the reporting period, 40 staff from all DHS Components were trained.

- **Reports Officer Certification Course**: The Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program. During the reporting period, the Office trained 16 reports officers on privacy policy.

[16] 10 DHS offices and components have a Privacy Officer.

B. DHS Privacy Office Awareness & Outreach

Publications

In February 2014, the DHS Privacy Office published the *2013 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

- 16th Plenary Negotiation of the US - EU Data Protection and Privacy Agreement (DPPA) – On December 16 -17, 2013, in Brussels, Belgium, the Chief Privacy Officer and the Director of International Privacy Policy represented the DHS Privacy Office as part of the U.S. delegation. The negotiation focused on the protection of data exchanged for law enforcement and homeland security purposes.

- NIST 800-53 Appendix J and Privacy Best Practices – On December 18, 2013, the Senior Director for Privacy Oversight represented the DHS Privacy Office at the National Institute of Standards and Technology (NIST) along with the Office of the Privacy Commissioner of Canada staff to discuss NIST 800-53 Appendix J and Privacy Best Practices. The purpose of the meeting was to provide an overview of how Appendix J started and how agencies are expected to use it. The Privacy Commissioner's Office is developing high-level guidance on privacy controls to integrate the Privacy Impact Assessment process with the government's security assessment processes, and plans to announce its guidance in May 2014.

- Privacy Advocates Meeting – On January 7, 2014, the Chief Privacy Officer met with representatives of the privacy advocacy community. The Senior Director of Privacy Compliance provided an overview of the DHS Data Framework, and the Senior Advisor for Privacy and Intelligence discussed Unmanned Aircraft Systems.

- Senate Homeland Security and Governmental Affairs Committee (HSGAC) – On January 14, 2014, the Chief Privacy Officer met with staff members of the HSGAC to provide an update on various privacy issues.

- Five Country Conference (FCC) Privacy and Informed Consent Working Group – On January 14, 2014, DHS Privacy Office staff participated in the inaugural meeting of an FCC working group charged with analyzing the legal, policy and regulatory frameworks of the five countries in support of privacy-compliant cross border data sharing among the FCC partners. These meetings of representatives from each of the FCC members will occur monthly, with the goal of producing recommendations to the principals at the 2014 Plenary.

- Canada School of Public Service Seminar for Senior Executives – On January 29, 2014, the Chief Privacy Officer participated in a panel discussion on privacy before a group of visiting Canadian officials as part of a Canada School of Public Service Seminar for Senior Executives on How Washington Works. The Chief Privacy Officer described the DHS privacy framework, highlighting how privacy policy is established in the United States in light of the changing technological landscape.

- Data Privacy and Integrity Advisory Committee (DPIAC) Meeting – On January 30, 2014, the Privacy Office hosted a public meeting of the DPIAC both online and in its District of Columbia office. The Chief Privacy Officer briefed committee members on DHS Privacy Office activities since the last meeting in September 2013, and provided her vision for the office going forward. The Senior Director of Privacy Compliance led a discussion on "big data" and three existing pilot programs. The Chief Privacy Officer tasked the committee with researching ways to improve transparency and oversight with respect to the DHS Data Framework.

- Federal Aviation Administration Second Annual National Data Privacy Symposium – On January 28, 2014, the Senior Director for Privacy Oversight participated on a panel entitled "Privacy - Align, Design, Refine," where she presented on implementation of NIST 800-53 Appendix J privacy controls. The Deputy Chief Privacy Officer also participated and gave a presentation on the Federal CIO Council Privacy Committee, its work within the CIO Council, and how that influences its priorities.

- RSA Conference – On February 26, 2014, in San Francisco, the Chief Privacy Officer participated on a panel entitled "Watching the Watchers: The New Privacy Officers Inside the U.S. Government."

- Data Protection and Privacy Agreement (DPPA) Plenary Session: On February 25 and 26, 2014, in Athens, Greece, DHS Privacy Office staff participated in a negotiation session of the DPPA, supporting the Offices of the General Counsel and International Affairs. Representatives from the Departments of State, Justice, and Treasury Department also participated.

C. Component Privacy Office Awareness & Outreach

National Protection and Programs Directorate

- Hosted a Privacy and Technology Workshop for all staff in the National Capital Region on December 5, 2013. Participants received technology demonstrations and learned about topics such as privacy, IT security, biometrics, and tools to protect from malware, cyber stalking, and spear phishing.

- Hosted Privacy and Acquisitions training at the Office of Infrastructure Protection Contracting Officer Representative Quarterly Meeting on February 5, 2014, providing a brief overview of NPPD's core privacy provisions, followed by a discussion of a privacy incident case study involving acquisitions-related activities.

- Provided privacy training to the Office of Infrastructure Protection, Information Security Compliance Division on February 24, 2014. The training focused on the protection of stakeholder contact information.

- Published an article in the employee newsletter, *NPPD Vision*, providing guidance on protecting sensitive information when working with industry contacts or potential vendors prior to an official procurement.

Office of Intelligence and Analysis

- Trained over 250 staff at an annual Intelligence Oversight course. A significant portion of the course covers the Privacy Act as well as privacy awareness best practices.

Transportation Security Administration

- Sent two all-staff email messages to raise privacy awareness; one on credit monitoring and one on how to protect medical information.

United States Citizenship and Immigration Services

- Developed procedures for identifying, tracking and reporting Local Developed Applications (LDA) to ensure that all LDAs that use, collect, maintain, or share PII have appropriate privacy compliance documentation in place.

- Collaborated with the USCIS Performance Management Branch to add language to employee performance evaluation guidance for management regarding PII. This language states that no PII should be included in the comments section of a performance evaluation, including redacted PII, otherwise this will be considered a privacy violation.

- Hosted an International Data Privacy Day on January 28, 2014, in the Northeast regional office, which included a presentation on *Privacy Risks Associated with Big Data*.

- Hosted a webinar in which the Central Region Privacy Officer briefed management on the new DHS Privacy Threshold Analysis (PTA) template, and how this template will be used.

- Published the USCIS Office of Privacy first quarter newsletter for Fiscal Year 2014 entitled, "*Privacy Chronicles*," to promote privacy awareness across USCIS.

- Published a *Privacy Tip* focused on the most recent change to the USCIS email policy allowing Alien Registration Numbers to be sent internally without being encrypted, due to the increased encryption implemented on the USCIS network.

United States Coast Guard

- Provided training on how to conduct and prepare a PTA to over 75 Information System Security Officers on January 16, 2014.

United States Immigration and Customs Enforcement

- Presented at the ICE Homeland Security Investigations, Office of Intelligence Basic Intelligence Training Course on January 31, 2014, discussing disclosures under the Privacy Act, proper handling of Sensitive PII, and privacy incidents.

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[18]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	1	2	0	3
Redress	0	0	0	0
Operational	860	1029	63	22
Referred	6	6	0	0
Total	***867***	***1037***	***63***	***25***

.

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.[19]
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.

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

[18] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

[19] 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.

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 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

Complaint: The complainant was stopped at a Canadian border checkpoint and asked to explain the reason for the visit to Canada. The complainant was informed that a misdemeanor traffic violation in 2004 had resulted in the complainant's name being placed on a watch list at the Canadian border. The complainant requested that Canada remove his name from the Canadian watch list.

***Disposition*:** The TSA Privacy Office advised that TSA is unable to determine why Canada questioned his entry into Canada or assist in removing his name from the Canadian watch list. The complainant was provided the link (http://www.cbsa-asfc.gc.ca) to the Canadian equivalent of CBP to resolve the situation, as well as referred to the state where the misdemeanor occurred to resolve the situation.

United States Customs and Border Protection

Complaint 1: The CBP INFO Center was contacted by a complainant who is a member of Global Entry (GE), a CBP Trusted Traveler Program, because the name on the Global Entry Card (assigned as a unique identifier) was not the true and correct name provided on the GE membership application. When the complainant sought assistance from the GE Help Desk and the GE Enrollment Center, they were unable to provide assistance. The complainant then contacted the CBP INFO Center for assistance in correcting the erroneous GE card.

***Disposition*:** The CBP INFO Center contacted the GE Trusted Traveler Program Office at CBP Headquarters and provided the GE traveler's correct full name, date of birth, and passport number as it should appear on the Global Entry card. The Trusted Traveler Program at CBP Headquarters confirmed the corrected information on the Global Entry account and sent the complainant a new Global Entry card. The CBP INFO Center then reached out to the complainant to advise that the Global Entry card had been corrected, a new card was issued, and it would be received in the mail.

Complaint 2: The CBP INFO Center was contacted by a complainant who reported that during a previous admittance to the U.S., her biometric fingerprints were transposed with her husband's. Since that time, the complainant reports that every time she and her husband enter the U.S., they are referred to secondary examination where the issue is quickly resolved and they are admitted to the U.S. The complainant contacted the CBP INFO Center to request assistance to permanently correct the biometric fingerprint problem.

***Disposition*:** The CBP INFO Center contacted the Passenger Service Manager at the District Field Office to investigate the matter. The District Field Office resolved the issue so that the complainant is admitted to the U.S. without being referred to secondary.

VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from December 1, 2013 – February 28, 2014. The DHS Privacy Office will continue to work with the Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.