Privacy Office

Third Quarter Fiscal Year 2011 Report to Congress

Department of Homeland Security Report of the Chief Privacy Officer Pursuant to Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*

August 2, 2011

Homeland Security

I. FOREWORD

August 2, 2011

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Third Quarter Fiscal Year 2011 Report to Congress*. This quarterly report includes activities from March 1, 2011 – May 31, 2011.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53, 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;
- Number and nature of privacy complaints received by DHS for alleged violations along with a summary of the disposition of such complaints; and
- Privacy training and awareness activities conducted by the Department to help reduce privacy incidents and increase adoption of our privacy risk management framework.

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") [Public Law 107-296; 6 U.S.C. §142], as amended. The mission of the DHS Privacy Office is to sustain privacy protections and to promote transparency of government operations while achieving the mission of the Department. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act,[1] the *Privacy Act of 1974*,[2] the *Freedom of Information Act* (FOIA),[3] the *E-Government Act of 2002*,[4] and the numerous laws, executive orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personally identifiable information (PII) collected, used, maintained, or disseminated by DHS.

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

The Honorable Joseph R. Biden
President, United States Senate

The Honorable John Boehner
Speaker, U.S. House of Representatives

[1] 6 U.S.C. § 101 *et seq.*
[2] 5 U.S.C. § 552a *et seq.*, as amended.
[3] 5 U.S.C. § 552
[4] 44 U.S.C. § 3501

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 at www.dhs.gov/privacy.

Sincerely,

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

DHS PRIVACY OFFICE
THIRD QUARTER FY 2011
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53, 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 information technology (IT) systems and programs that may have a privacy impact. For purposes of Section 803 reporting, reviews include the following activities:

1. Privacy Threshold Analyses (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*, the *Homeland Security Act of 2002*, as amended, by policy or other law;
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, which provide notice to individuals at the point of collection;
5. Computer Matching Agreements;
6. Data Mining Report as defined by Congress under Section 804 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*; and
7. Privacy reviews of IT and program budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board.

Q3 FY2011 Reviews	
Review Type	**# of Reviews**
Privacy Threshold Analyses	158
Privacy Impact Assessments	22
System of Records Notices and Associated Privacy Act Exemptions	8
Privacy Act (e)(3) Statements	6
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews	***194***

Privacy Impact Assessments
The PIA process is one of the key mechanisms used to assure that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. As of May 31, 2011, 76 percent of the Department's Federal Information Security Management Act (FISMA) systems that require a PIA are currently covered by a PIA. Additionally, the Department has implemented a triennial review program for legacy PIAs to assess and confirm that these systems are still operating within the originally published parameters. As these systems are renewed, notification will be added to the previously published PIA to inform the public that a review has been conducted for that system. A complete list of PIAs conducted by DHS can be found on our website. The following are six examples of the 22 PIAs published during this reporting period:

- ***DHS/USCIS/PIA-036, E-Verify Self Check*** - The U. S. Citizenship and Immigration Services (USCIS) Verification Division has developed a new service called E-Verify Self Check. This voluntary service is available to individuals who want to check their work authorization status prior to employment and correct any errors in federal databases that provide inputs into the E-Verify process. When an individual uses the E-Verify Self Check service, he or she will be notified that either: 1) his or her information matched information contained in federal databases and would be deemed work-authorized; or 2) his or her information was not matched to information contained in federal databases, which would be considered a "mismatch." If information is a mismatch, he or she will be instructed on where and how to correct the record. USCIS conducted this PIA because E-Verify Self Check will collect and use PII. (*March 4, 2011*)

- ***DHS/ALL/PIA-036, Use of Unidirectional Social Media Applications*** - This PIA analyzes the Department's use of unidirectional social media applications but does not cover users sending content to the Department. DHS uses unidirectional social media tools including desktop widgets, mobile apps, podcasts, audio and video streams, Short Message Service (SMS) texting, and Really Simple Syndication (RSS) feeds, among others, for external relations and to disseminate timely content to the public about initiatives, public safety, and other official activities and one-way notifications. These dynamic communication tools broaden the Department's ability to disseminate content and provide the public with multiple channels to receive and view content. The public will continue to have the option to obtain comparable content and services through the Department's official websites and other official means. Additionally, this PIA describes the extremely limited circumstances when the Department will have access to PII, how it will use PII, what PII is retained and shared, and how individuals can gain access to their own PII. (*March 8, 2011*)

- ***DHS/FEMA/PIA-016, Application and Registration Records for Training and Exercise Programs (ARRTEP)*** - The Federal Emergency Management Agency (FEMA) sponsors, hosts, and conducts numerous training and exercise programs in support of its mission. These programs collect PII from individuals who register to participate in these programs. This PIA covers programs that collect basic PII but do not require sensitive PII such as Social Security numbers, dates of birth, and financial and medical information for registration purposes. (*March 3, 2011*)

- ***DHS/USCG/PIA-016, College Board Requirement Plus (CBRP)*** - The United States Coast Guard Academy (USCGA) uses College Board's *Recruitment PLUS*™ software application for college admissions and enrollment activities. The Recruitment PLUS system: collects and stores prospective applicants' biographic and educational data; collects USCGA admissions staff and volunteers' biographical data; facilitates and tracks the application process; and aligns admissions staff and volunteers to prospective applicants. The purpose of this PIA is to document how Recruitment Plus collects and uses PII. (*April 1, 2011*)

- ***DHS/ALL/PIA-037, SharePoint and Collaboration Sites*** - DHS is developing SharePoint as a Service (SharePoint), an enterprise-wide offering available to all organizations within the Department. This platform will serve as a collaboration and communication solution, eliminating additional investments in duplicative collaborative technologies, leveraging economies of scale, and connecting separate organizations through the use of a shared platform in an integrated environment. DHS is conducting this PIA because PII may be collected and stored in the SharePoint environment. This PIA sets the minimum standard for SharePoint privacy and security requirements; DHS components may build more detailed controls and technical enhancements into their respective sites. (*March 22, 2011*)

- ***DHS/ALL/PIA-038, Integrated Security Management System (ISMS)*** - The Integrated Security Management System (ISMS) is a web-based case management tool designed to support the lifecycle of DHS personnel security, administrative security, and classified visit management programs. Personnel security records maintained in ISMS include suitability and security clearance investigations which contain information related to background checks, investigations, and access determinations. For administrative security and classified visit management, ISMS contains records associated with security container/document tracking, classified contract administration, and incoming and outgoing classified visitor tracking. This system is a DHS enterprise-wide application that replaces the Personnel Security Activities Management System, which was decommissioned on May 31, 2010. (*March 22, 2011*)

System of Records Notices

In addition to the PIAs published during this reporting period, DHS also published eight Privacy Act SORNs to support systems at the Office of Health Affairs (OHA), Office of Operations Coordination and Planning (OPS), Science and Technology (S&T), Federal Emergency Management Agency (FEMA), and the United States Coast Guard (USCG). As of May 31, 2011, 95 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. SORNs continue to 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 valid. The following are three examples of SORNs that were published during the reporting period and can be found on our website:

- ***DHS/OPS-002, National Operations Center Tracker and Senior Watch Officer Logs System of Records*** – DHS/OPS National Operations Center Tracker Log (NOC Log) is the underlying cumulative repository of responses to all-threats and all-hazards, including acts of terrorism and natural disasters, and requests for information that require a NOC tracking number. The NOC tracker numbers are used in a wide variety of products originated by the Department or external sources. They are shared inside and outside of the Department and serve as shorthand for tying data used in internal and external reports and agency actions to the event that caused them. The NOC Log contains a copy of all documents and information that is requested, shared, and/or researched between all NOC Watch Officer Desks. Because of the depth and breadth of information that the NOC receives, categories of individuals and records are broad so as to cover the possibility of this PII entering this Privacy Act system of records within the NOC. (*March 8, 2011*)

- ***DHS/USCG-007, Special Needs Program System of Records*** – The USCG developed this system to meet its obligation to assist military personnel, civilian personnel and their eligible dependents with special needs. As a result of the required biennial review of this system, records have been updated to reflect the name change to DHS/USCG Special Needs Program Record. This updated system will be included in the Department's inventory of records systems. (*May 3, 2011*)

- ***DHS/S&T-.0001, Safety Act Records Consolidation System of Records*** – The Science and Technology Directorate is consolidating a SORN from its inventory of records systems titled, *DHS/Directorate of Science and Technology (S&T)-.0001 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002*, (68 FR 55642, September 26, 2003), into the existing DHS SORN titled, *DHS/ALL-002, Mailing and Other Lists System*, (73 FR 71659, November 25, 2008). This system was established to maintain records on individuals who submit applications for technologies seeking liability protection under provisions of the *Support Anti-Terrorism by Fostering Effective Technologies Act*. Since these records are limited to individuals' contact information (business phone number, mailing address, e-mail address), DHS has determined this system can be covered under the *DHS/ALL-002, Mailing and Other Lists System* SORN. Consolidating this SORN will have no adverse impact on individuals, but will promote the overall streamlining and management of DHS Privacy Act record systems. (*April 18, 2011*)

IV. ADVICE AND RESPONSES

Privacy Training, Awareness and Outreach

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

- **6,391** DHS personnel attended instructor-led privacy training courses.
- **51,801** DHS personnel and contractors completed the mandatory computer-assisted privacy training course, *Culture of Privacy Awareness* (note: this is an annual requirement).

New Employee Training

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

Fusion Center Training

- During this reporting period, the DHS Privacy Office continued to collaborate with the Office of Intelligence and Analysis and the Office for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to staff at fusion centers.
- The DHS Privacy Office also provides training to intelligence professionals selected for assignment to fusion centers from I&A, as required under section 511 of the *9/l1 Commission Act*.
- The total number of fusion center staff trained in this reporting period is reported in the Section 803 Report for the DHS Office for Civil Rights and Civil Liberties.

A. DHS Privacy Office Awareness & Outreach

Publications

This is a list of publications written or collaborated on by DHS Privacy Office staff. Most can be found on our website, www.dhs.gov/privacy.

- *DHS Policy and Procedures for Managing Computer-Readable Extracts (CREs) Containing Sensitive PII*, an addendum to *DHS 4300A, Sensitive Systems Handbook*. This draft addendum was written by DHS Privacy Office staff to provide direction to DHS offices, Components, and personnel on creating and managing CREs that contain sensitive PII. (updated March 2011.)
- *Attachment X—Social Media* (May 2011), an addendum to *DHS 4300A, Sensitive Systems Handbook*. This document provides information security guidance regarding official and unofficial social media use occurring within or outside of the DHS network.
- *Fact Sheet: "How to Safeguard Personally Identifiable Information"* (May 2011). This updated fact sheet conveys best practices to protect sensitive PII at the Department.

Meetings & Events

- Panel on Transatlantic Privacy – On March 3, 2011, the Chief Privacy Officer participated on a panel discussion on *Privacy and Data Protection*. The event was part of the Sixth Annual American Bar Association Homeland Security Law Institute.

- American Society of Access Professionals (ASAP) Conference – On March 7 – 9, 2011, the Associate Director of Freedom of Information Act (FOIA) Policy and Program Development spoke on four separate panels at the ASAP National Training Conference in Las Vegas, Nevada. The presentations reviewed selected FOIA exemptions along with how to work with FOIA requesters and contractors.
- International Association of Privacy Professionals (IAPP) – On March 10, 2011, two Privacy Office employees spoke at the largest privacy conference in the U.S. The Chief Privacy Officer participated in a panel on suspicious activity reporting (along with ACLU and the National SAR Initiative) entitled: *Did You See and Say Something? What Does the Government Do With That Information?* The Senior Privacy Analyst for Information Sharing also participated on the National Strategy on Trusted Identities in Cyberspace (NSTIC) panel along with the Department of Commerce, National Security Staff, and NIST.
- Data Privacy and Integrity Advisory Committee Meeting (DPIAC) – On March 9, 2011, the DPIAC held its first 2011 quarterly public meeting. The agenda included an update by the Chief Privacy Officer on Privacy Office activities and a briefing by Howard Schmidt, Special Assistant to the President and Cybersecurity Coordinator for the Federal Government, on the Obama Administration's cybersecurity efforts. The Associate Director for Privacy Compliance gave a brief overview on privacy protections built into the Department's use of social media. The meeting minutes and transcript are posted on the Privacy Office's website.
- 2011 National Fusion Center Conference – March 14 – 17, 2011, the Chief Privacy Officer, along with the Director of Legislative and Regulatory Analysis and a Senior Privacy Analyst, attended the National Fusion Center Conference in Denver, Colorado. The Chief Privacy Officer participated on a panel entitled *Building a Fusion Center Culture that Shares Information while Protecting Privacy and Civil Liberties*.
- Privacy Information for Advocates Meeting – On March 18, 2011, the Chief Privacy Officer hosted the quarterly Privacy Information for Advocates meeting, which is designed to proactively engage the privacy community on privacy issues.
- Committee on Women in the Profession: Women in IP Breakfast Series - *Hot Topics in Privacy* – On April 26, 2011, the Chief Privacy Officer participated as a speaker at the Women in IP Breakfast Series in New York, sponsored by the New York City Bar Association.
- Microsoft Innovation Outreach Partnership (IOP) Privacy Conference – On April 26, 2011, the Chief Privacy Officer participated as a keynote speaker at the IOP conference in New York. She gave a presentation entitled: *Government Approach to Innovation and Privacy,* sponsored by IOP & WorldTech International, LLC.
- American University - Washington College of Law Academic Conference – On April 27, 2011, Associate Director of FOIA Policy and Program Development participated on a panel discussion entitled, "*High Noon for High 2…and Beyond*" at an American University - Washington College of Law academic conference on the protection of Homeland Security information.
- RISE Washington Conference – On May 5, 2011, the Chief Privacy Officer made a keynote presentation during dinner at the RISE Washington Conference on Biometrics and Security in the Global Perspective (sponsored by the Center for Policy on Emerging Technologies). The Director of Privacy Policy was a discussant on May 6 for an associated roundtable.
- DPIAC Meeting – On May 19, 2011, the DPIAC held a public meeting by teleconference. The agenda included a report from the Chief Privacy Officer on Privacy Office activities since the DPIAC's March 2011 meeting, and a briefing by the Privacy Officer for the Science & Technology Directorate (S&T) on S&T's implementation of privacy policy.

B. Component Privacy Office Awareness & Outreach

Federal Law Enforcement Training Center Privacy Office
April 13-14, 2011, the International Privacy Policy Director participated in a curriculum development session led by FLETC for pre-deployment training for DHS employees posted overseas. The DHS Privacy Office supports FLETC in its effort to develop a formal training program for DHS international officers and attaches and will ensure that international privacy equities are included, as appropriate.

National Protection and Programs Directorate Privacy Office
- In May 2011, *US-VISIT Today* ran a privacy tip entitled "*Protect YOUR Privacy – Fight Back Against Identity Theft!*" to remind all employees to safeguard their personal information.
- On May 5, 2011, the Senior Privacy Officer briefed eleven of NPPD's field Site Security Officers on general privacy compliance requirements, as well as on recommended privacy practices to prevent data breaches.
- On May 6, 2011, the Director of US-VISIT gave the opening keynote address at the Biometrics and Security in Global Perspective Conference.

Transportation Security Administration Privacy Office
- Distributed a WIFI-related broadcast to TSA personnel as a public service announcement.
- Continued to enhance privacy awareness by contributing guidance to the Office of Intelligence, Office of Threat Assessments and Credentialing, Information System Security Officers, and the Office of Transportation Sector Network Management.

U.S. Citizenship and Immigration Services Privacy Office
On April 5, 2011, the Chief Privacy Officer gave the keynote address to kick-off the first-ever Privacy Awareness Week at USCIS. The International Privacy Policy Director also participated as a speaker, highlighting the international privacy developments and the role of U.S. privacy law and DHS privacy policy. Other speakers included: Marc Groman, Chief Privacy Officer for the Federal Trade Commission; John Mazza, Special Agent, United States Secret Service; and Charlene Thomas, Senior Advisor for Privacy Policy at the Department of State.

U.S. Citizenship and Immigration Services Verification Division Privacy Office
On May 17, 2011, the Deputy Chief Privacy Officer presented a privacy overview to kick off the annual e-Verification Privacy Awareness Week. He was joined by a Privacy Analyst who presented an overview of Cloud Computing.

U.S. Immigration & Customs Enforcement Privacy Office
- Emailed a privacy tip to all employees.

U.S. Secret Service Privacy Office
- Issued posters and flyers to raise privacy awareness and encourage employees to protect PII.
- Launched an official Twitter page to promote transparency and proactive disclosure, and supplement ongoing efforts to educate the public on the mission of the Secret Service.
- Established a privacy e-mail account for employees to submit questions and/or comments regarding privacy compliance and how to safeguard PII, and also to report 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 Act and Privacy Management*. Complaints are received from U.S. citizens, Legal Permanent Residents, visitors, or aliens.[5]

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	4	2	0
Redress	4	4	0	2
Operational	283	278	27	6
Referred	2	1	1	1
Total**	***295***	***287***	***30***	***9***

*This category may include responsive action taken on a complaint received from a prior reporting period.
**The total reflects a difference of one complaint that was closed in a prior reporting period but not accounted for at that time.

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, correction of PII, and redress therein.
   Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[6]
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 they must first be resolved with the external entity.

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

Transportation Security Administration
The TSA Privacy Office received a complaint from an employee who believed TSA personnel had mishandled medical information attached to a leave request. The employee expressed concern that the individuals tasked to input the data at the facility did not have a need to know the information in the performance of their official duties. After investigating the situation, the TSA Privacy Office determined that the individuals assigned to process the leave request did have a need to know the information to assist in the approval process. As a result of this determination, the employee subsequently rescinded his complaint.

U.S. Citizenship and Immigration Services
The USCIS Privacy Office received a complaint from an employee in a field office. The employee complained that management improperly handled PII belonging to staff participating in the Transportation Subsidy Program. Specifically, the employee stated that management had collected the names and mothers' maiden names of each employee participating in the transit subsidy program and sent it to a bank that had requested the information as part of the program. The employee believed this bank should have requested and obtained the PII from each employee directly, and not from USCIS staff. The USCIS Privacy Office investigated the issue and determined that management received a letter from the bank indicating they needed the PII to validate employees when they subsequently went to retrieve their transit subsidies. To help expedite the process, management collected the PII and submitted it to the bank on an encrypted CD. The USCIS Privacy Office noted that management did not keep a copy of the PII after sending it to the bank.

The USCIS Privacy Office determined that management did not violate employee privacy rights or mishandle employee PII. Management made a discretionary decision to expedite the information collection to ensure that all employees continued to receive their transportation subsidy without interruption. The action was found to be well within management's rights.

U.S. Customs and Border Protection
An email was received from a traveler who stated that, upon arriving at Miami International Airport, he was taken to a secondary screening room where he was interviewed and his luggage inspected. He alleged that his Fourth Amendment privacy rights were violated during the screening because: (1) a CBP officer read papers that were in his wallet; and (2) such a thorough inspection must be illegal. A response was sent explaining CBP's search authority, citing 19 C.F.R. 162.6, as well as an apology for any rude or unprofessional behavior that may have occurred during the screening process. The complainant was satisfied with the response.

U.S. Visitor and Immigrant Status Indicator Technology
US-VISIT was informed by a woman that she had experienced problems at an airport because of a possible mismatch in the IDENT system. US-VISIT reviewed her record in the IDENT system and found the mismatch. Her biometrics (fingerprints) had inadvertently been attached to another individual's record, and vice versa. US-VISIT corrected the information in both records.