



Department of Homeland Security

Privacy Office

Fourth Quarter Fiscal Year 2012 Report to Congress

December 18, 2012



Homeland
Security

I. FOREWORD

December 18, 2012

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Fourth Quarter Fiscal Year 2012 Report to Congress*. This quarterly report covers activities from June 1, 2012 – August 31, 2012.¹



Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*² (*9/11 Commission Act*) requires the DHS Privacy Office to report quarterly on the 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 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. Section 222 of the *Homeland Security Act of 2002* (“Homeland Security Act”), as amended,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 (FOIA), 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, this report is being provided to the following Members of Congress:

The Honorable Joseph I. Lieberman

Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins

Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy

Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley

Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein

Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss

Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Peter T. King

Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson

Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Darrell Issa

Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings

Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Lamar Smith

Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.

Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Mike Rogers

Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C. A. Dutch Ruppersberger

Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

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, listed below.

Sincerely,



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



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

Table of Contents

I.	FOREWORD	1
II.	LEGISLATIVE LANGUAGE	5
III.	PRIVACY REVIEWS.....	6
	A. Privacy Impact Assessments.....	8
	B. Systems of Record Notices	12
	C. Privacy Compliance Reviews	13
IV.	ADVICE AND RESPONSES.....	14
	A. Privacy Training and Awareness	14
	B. DHS Privacy Office Awareness & Outreach	15
	C. Component Privacy Office Awareness & Outreach	16
V.	PRIVACY COMPLAINTS AND DISPOSITIONS.....	18
VI.	CONCLUSION	20

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 of 2002*, the *Homeland Security Act of 2002*,⁷ and DHS policy;
3. System of Records Notices (SORN) as required under the *Privacy Act of 1974*⁸ and associated *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 Privacy Office by the *Homeland Security Act of 2002*;
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. § 552 (Note).

¹² 42 U.S.C. § 2000ee-3.

**Table I:
Reviews Conducted During
Fourth Quarter Fiscal Year 2012**

Review Type	Number of Reviews
Privacy Threshold Analyses	171
Privacy Impact Assessments	26
System of Records Notices and Associated <i>Privacy Act</i> Exemptions	7
<i>Privacy Act</i> (e)(3) Statements	17
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests	99
Other Privacy Reviews	0
<i>Total Reviews</i>	322

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 for the use, collection, and disclosure of PII. As of August 31, 2012, 85 percent of the Department's Federal Information Security Management Act (FISMA) systems requiring a PIA had a PIA 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.

The Department published 26 new or updated PIAs during this reporting period, and a sample of them are summarized below. Updates to existing PIAs appear with a lower-case letter in parentheses after the original PIA number. All PIAs are available on our website, www.dhs.gov/privacy.

DHS/ALL/PIA-014(b) - Personal Identity Verification (PIV) Management System Update

Background: The Department updated its Personal Identity Verification (PIV) PIA update, originally issued on June 18, 2009, to reflect changes in Departmental requirements and enhanced interoperability with the following: US-VISIT Automated Biometric Identification System (IDENT), the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Integrated Automated Fingerprint Identification System (IAFIS), DHS Component Physical Access Control Systems (PACS), DHS Component Active Directories, and PIV-compatible credentials for DHS visitors.

Purpose: This PIA update details the new interaction between the IDMS and DHS Component Active Directory and PACS, and the US-VISIT IDENT system. (*August 23, 2012*)

DHS/CBP/PIA-006(b) - Automated Targeting System (ATS) Update

Background: U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS). As a decision support tool, ATS compares traveler, cargo, and conveyance information against law enforcement and intelligence data using risk-based targeting scenarios and assessments.

Purpose: This PIA update informs the public about changes in modules and expansion of access to datasets used by and stored in ATS. This PIA was published in conjunction with an updated System of Records Notice (SORN) in the *Federal Register*. (*June 1, 2012*)

DHS/CBP/PIA-007(b) - Electronic System for Travel Authorization (ESTA) - Internet Protocol Address and System of Records Notice Update

Background: ESTA is a web-based application and screening system used to determine if certain aliens are eligible to travel to the United States under the Visa Waiver Program.

Purpose: This PIA update evaluates the privacy impacts of: (1) including the Internet Protocol address associated with a submitted ESTA application for vetting purposes; and (2) various updates to the ESTA System of Records Notice (SORN), including updates and clarifications to the existing routine uses, along with a new routine use permitting the sharing of information about judicial proceedings. (*July 18, 2012*)

DHS/CBP/PIA-010 – Analytical Framework for Intelligence (AFI)

Background: AFI enhances DHS' ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk. AFI also aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border.

Purpose: CBP conducted this PIA because AFI accesses and stores PII retrieved from DHS, other federal agencies, and commercially available databases. *(June 1, 2012)*

DHS/CBP/PIA-012 – CBP Portal (E3) to ENFORCE/IDENT

Background: CBP has established E3, its portal to U.S. Immigration and Customs Enforcement's (ICE) Immigration and Enforcement Operational Records System (ENFORCE), Enforcement Integrated Database (EID), and US-VISIT's Automated Biometric Identification System (IDENT), in order to collect and transmit data related to law enforcement activities.

Purpose: CBP conducted this PIA because E3 collects and transmits biographic, encounter, and biometric data including fingerprints for the identification and verification of individuals encountered at the border. *(July 25, 2012)*

DHS/FEMA/PIA-025 – Hazard Mitigation Grant Program (HMGP) System

Background: The Federal Emergency Management Agency's (FEMA) Federal Insurance and Mitigation Administration (FIMA) operates the Hazard Mitigation Grant Program (HMGP) system, a grant application and management system.

Purpose: FEMA conducted this PIA because FEMA's FIMA HMGP system may collect, use, maintain, retrieve, and disseminate the PII of grantees or sub-grantees, as well as that of property owners associated with grants and sub-grants. *(June 28, 2012)*

DHS/FEMA/PIA-027 – National Emergency Management Information System-Individual Assistance (NEMIS-IA) Web-based and Client-based Modules

Background: FEMA's Office of Response and Recovery (OR&R), Recovery Directorate, National Processing Service Center (NPSC) Division operates the National Emergency Management Information System (NEMIS) Individual Assistance (IA) system. NEMIS-IA processes information obtained from disaster recovery assistance applications via the Disaster Assistance Improvement Program /Disaster Assistance Call Center system. NEMIS-IA includes both client-based and web-based modules and works to detect and prevent the duplication of benefits.

Purpose: FEMA conducted this PIA because NEMIS-IA collects, uses, maintains, retrieves, and disseminates the PII of applicants to FEMA's disaster recovery individual assistance programs. *(June 29, 2012)*

DHS/ICE/PIA-010(a) - National Child Victim Identification System (NCVIS)

Background: The National Child Victim Identification System (NCVIS), owned by ICE Homeland Security Investigations (HSI), assists authorized partners, including federal, state, local, and international law enforcement agencies, INTERPOL, and organizations such as the National Center for Missing and Exploited Children, in the investigation and prosecution of child exploitation crimes, specifically those involving images of child sexual exploitation. HSI is expanding the scope of system information shared with authorized partners for the purposes of identifying victims and supporting criminal law enforcement investigations and prosecutions.

Purpose: ICE published the original PIA for NCVIS on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, ICE completed an update to the PIA. *(July 17, 2012)*

DHS/ICE/PIA-015(e) - Enforcement Integrated Database ENFORCE - EAGLE Update

Background: ICE has established a new subsystem within the Enforcement Integrated Database (EID) called the EID Arrest Graphic User Interface for Law Enforcement (EAGLE). EAGLE is a booking application used by ICE law enforcement officers to process the biometric and biographic information of arrested individuals. When fully deployed, EAGLE will replace the existing EID booking applications, including the Enforcement Apprehension and Booking Module (EABM), Mobile IDENT, and WebIDENT, and will perform the identical functions of those applications. EAGLE will also forge a new connection with the Department of Defense's (DOD) Automated Biographic Information System (ABIS) and permit the comparison of the fingerprints of foreign nationals arrested by ICE with the DOD's information in ABIS.

Purpose: This PIA update informs the public about the operation of the EAGLE booking system and its connection to the DOD ABIS database. *(July 25, 2012)*

DHS/NPPD/PIA-021 - Joint Cybersecurity Services Program, Defense Industrial Base - Enhanced Cybersecurity Services

Background: The Joint Cybersecurity Services Pilot (JCSP) is the Department's voluntary information sharing initiative with DOD and participating commercial companies. The National Protection and Programs Directorate (NPPD) updated the National Cyber Security Division Joint Cybersecurity Services Pilot PIA, originally published on January 13, 2012, to reflect the establishment of the JCSP as an ongoing permanent program (now known as the Joint Cybersecurity Services Program). The program enhances the cybersecurity of participating critical infrastructure entities through information sharing partnerships with the critical infrastructure organization or their Commercial Service Provider. The first phase of the Program will focus on the cyber protection of Defense Industrial Base (DIB) companies that are participating in the DOD's Cyber Security/Information Assurance Program, known as the DIB Enhanced Cybersecurity Services.

Purpose: NPPD updated the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA published on January 13, 2012 to reflect the establishment of JCSP as an ongoing permanent program. *(July 18, 2012)*

DHS/NPPD/PIA-026 - National Cybersecurity Protection System (NCPS)

Background: The National Cybersecurity Protection System (NCPS) is an integrated system for intrusion detection, analysis, and prevention, as well as for information sharing capabilities used to defend the Federal Civilian Government's information technology infrastructure from cyber threats. The NCPS includes the hardware, software, supporting processes, training, and services that are developed and acquired to support its mission.

Purpose: This PIA was conducted because PII may be collected by the NCPS, or through submissions of known or suspected cyber threats received by the United States-Computer Emergency Readiness Team (US-CERT) for analysis. This PIA replaces previously published PIAs submitted by NSCD for the 24/7 Incident Handling Center (March 29, 2007), and the Malware Lab Network (May 4, 2010), and is a better focused PIA to characterize the efforts of NCPS and US-CERT. *(July 30, 2012)*

DHS/OPS/PIA-007 - HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network

Background: The DHS Office of Operations, Coordination and Planning (OPS) maintains the Homeland Security Information Network (HSIN) on the Sensitive but Unclassified (SBU) network. HSIN facilitates the secure integration and interoperability of information-sharing resources between federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners involved in identifying and preventing terrorism, as well as in undertaking incident management activities. HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas.

Purpose: OPS conducted this PIA because HSIN contains PII about HSIN users and members of the public who are the subject of documents, reports, or bulletins contained in the HSIN collaboration spaces. This PIA only covers the substantive material posted and shared within the HSIN collaboration spaces, and not the individual user accounts. *(July 25, 2012)*

DHS/OPS/PIA-009 - National Operations Center Operations Counterterrorism Desk (NCOD) Database

Background: The National Operations Center (NOC) within OPS operates the NOC Counterterrorism Operations Desk (NCOD). The NCOD Database is a tracking tool used by NCOD Officers to track all counterterrorism related inquiries.

Purpose: OPS conducted this PIA because the NCOD Database contains PII. *(July 31, 2012)*

DHS/USCIS/PIA-045 - Deferred Action for Childhood Arrivals (DACA)

Background: Deferred action is an exercise of the Secretary's prosecutorial discretion to defer removal action against certain individuals who came to the United States as children and meet several key guidelines on a case-by-case basis in order to focus enforcement resources on the removal of individuals who pose a danger to national security or public safety or have been convicted of specific crimes.

Purpose: USCIS conducted this PIA because the deferred action for childhood arrivals process associated with the Secretary's related memorandum involves the collection and use of PII.

B. System of Records Notices

As of August 31, 2012, 96 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.

DHS SORNs and Final Rules for Privacy Act Exemptions are available on our website, www.dhs.gov/privacy.

During the reporting period, DHS published six SORNs and one Final Rule for Privacy Act Exemptions, and a sample of them are summarized below.

DHS/USCIS - 006(a) Systematic Alien Verification for Entitlements (SAVE) Program System of Records

This system of records was updated by USCIS to provide notice that SAVE is: (1) adding the collection of the foreign passport country of issuance (COI) from the agencies that issue the benefits, and from US-VISIT's Arrival and Departure Information System (ADIS) to the "Categories of Records;" (2) moving the list of sources of records from "Category of Records" to "Record Source Categories;" (3) removing two decommissioned systems, and adding two new systems from "Record Source Categories;" (4) updating the system location information for the Verification Information System (VIS), the underlying technology supporting the SAVE program, from a contractor-owned facility to a government-owned facility ; (5) incorporating minor changes to the "Routine Uses" to improve clarity; and (6) adding COI to "Retrievability" as a way in which DHS may retrieve records in this system of records. This updated system is included in the DHS inventory of records systems. (*August 8, 2012, 77 FR 47415*)

DHS/USCIS - 044 Fraud Detection and National Security Directorate

This system of records assists USCIS in performing its statutory missions, including strengthening the integrity of the nation's legal immigration system, by ensuring that immigration benefits are not granted to individuals that may pose a threat to national security and/or public safety. In addition, this SORN assists USCIS in recording, tracking, and managing immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. This system of records is being updated to more clearly describe the functions of the Fraud Detection and National Security Directorate, and clarify that the system of records contains both electronic and paper files. (*August 8, 2012, 77 FR 47411*)

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 Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR 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 Agreements.

Reports on the results of PCRs are available on our website, www.dhs.gov/privacy.

During this reporting period, the DHS Privacy Office completed one PCR on a DHS-sponsored system for a classified, multi-agency, information sharing environment.

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

78,800 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

2,365 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 Officers¹³ also offer introductory privacy training for new employees.

Fusion Center Training

- The DHS Privacy Office collaborates with the Office of Intelligence and Analysis (I&A) and the Office for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to staff at state and major urban area fusion centers.
 - *During the reporting period, DHS trained 207 people in 4 sessions at 4 fusion centers.*

Reports Officer Training

- The DHS Privacy Office provides training to officers who prepare intelligence reports as part of a comprehensive Reports Officer Training Certification Course.
 - *During the reporting period, DHS trained 25 officers on privacy policy.*

Nationwide Suspicious Activity Reporting Initiative

- The DHS Privacy Office provides training to Suspicious Activity Reporting (SAR) analysts.
 - *During the reporting period, DHS trained 25 analysts on privacy issues related to suspicious activity reporting.*

¹³ Each of the 10 sub-Components that comprise the Department has a Privacy Officer.

B. DHS Privacy Office Awareness & Outreach

Outreach

Annual Privacy Compliance Workshop – On June 20, the DHS Privacy Office hosted its annual workshop, the only one of its kind, to train federal privacy practitioners on federal privacy compliance best practices. 270 people attended from 40 federal agencies.

Meetings & Events

- International Privacy Policy Training - On June 6, the International Privacy Programs Director briefed 30 Foreign Service Officers at the State Department’s Foreign Service Institute on international privacy policy issues.
- Privacy Information for Advocates Meeting – On June 16, the Chief Privacy Officer hosted a quarterly meeting to proactively engage the privacy community on current privacy issues.
- Beyond the Border (BTB) – On June 21, the Chief Privacy Officer attended a meeting of the Beyond the Border U.S.-Canada Executive Steering Committee in Ottawa, Canada, to discuss the BTB Joint Statement on Privacy Principles.
- Data Privacy and Integrity Advisory Committee (DPIAC) Meeting – On July 17, the DPIAC held a public meeting in Washington, DC. Following the Chief Privacy Officer’s update, the Committee received a briefing on Social Media Use for Situational Awareness from the Office of Operations Coordination and Planning, and the DHS Privacy Office, along with an overview of the U.S. Coast Guard’s Biometrics and Sea Program.
- Treasury Department’s Chief Information Officer (CIO) Council – On July 19, the Senior Director for Privacy Oversight gave a presentation on “New Draft NIST Special Publication 800-53, Appendix J” to 27 CIOs from various Treasury Department bureaus.
- Senate Testimony – On July 31, the Chief Privacy Officer testified on the state of federal privacy and data security law before the United States Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency (FEMA) Privacy Office

- Provided privacy awareness training to: (1) all new headquarters employees and contractors during new employee and new contractor orientations, and (2) personnel in Region V (Chicago).

National Protection and Programs Directorate (NPPD) Office of Privacy

- Provided role-based privacy training to NPPD Office of Legislative Affairs staff, with special emphasis on cybersecurity and disclosure of Privacy Act-protected records.
- Provided general privacy training to Office of Cybersecurity & Communications staff.
- Published a new issue of the *Privacy Update*, a quarterly publication aimed at increasing overall awareness of privacy, with a focus on educating employees about how to avoid and respond to incidents of identity theft.
- Spoke at the Federal CIO Council Privacy Committee, Best Practices Subcommittee meeting on how to plan a successful privacy awareness event in Washington, DC, on June 17.
- Assisted in organizing the Federal CIO Council Privacy Committee's Development and Education Subcommittee event, "Safeguarding Sensitive PII." 150 people attended the event at the Federal Trade Commission in Washington DC, on August 22.
- Published a privacy tip in NPPD's electronic newsletter about the threat of social engineering and the importance of using strong passwords. The US-VISIT Program also published three privacy tips in its online newsletter related to Smartphone security, strong passwords, and avoiding identity theft.
- Distributed guidance to employees on securing PII during office moves.

Transportation Security Administration (TSA) Privacy Office

- Presented on the privacy threshold analysis process at the DHS Privacy Office's Annual Privacy Compliance Workshop in Washington DC, on June 20.
- Presented DHS/TSA privacy policies to General Dynamics contractors involved in a technology procurement at TSA headquarters on August 28.

United States Citizenship and Immigration Services (USCIS) Privacy Office

- Presented at the Fraud Detection and National Security (FDNS) Basic Instructor Training to provide FDNS Immigration Analysts the skills needed to fulfill their roles in fraud detection and prevention and the identification of public safety and national security cases, in Burlington, Vermont, on July 25.
- Provided privacy awareness training to employees at the Mission Support Training in Burlington, Vermont, on August 27.
- Trained 24 employees on how to safeguard Sensitive PII at the Basic Records Academy Training Course in Washington, DC, on June 27-30.
- Conducted eight site visits to regional offices to perform privacy awareness training (multiple dates and locations).

U.S. Customs and Border Protection (CBP) Privacy Officer

- Trained senior officials to be Privacy Liaisons from the following offices: Field Operations, Border Patrol, International Trade, Information Technology, Internal Affairs, and Intelligence and Investigative Liaison. These Privacy Liaisons will serve two year terms identifying initial privacy issues for their office. Moving forward, each program office that also owns a privacy system shall designate one or more employees in their operational and/or program units to serve as a Privacy Liaison. Other CBP offices may designate a Privacy Liaison as needed.
- Presented on the Privacy Threshold Analysis process during the panel discussion, *The Life Cycle of DHS Privacy Compliance*, at the DHS Privacy Office's Annual Privacy Compliance Workshop in Washington, DC, on June 20.

U.S. Immigration and Customs Enforcement (ICE) Privacy Office

- Presented on how to properly analyze a SORN at the DHS Privacy Office's Annual Privacy Compliance Workshop in Washington, DC, on June 20.
- Presented on disclosures under *The Privacy Act* to the Homeland Security Investigations Fugitive Program Working Group in Washington, DC, on August 1.

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.¹⁴

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	2	3	0	2
Redress	0	2	0	0
Operational	693	633	76	13
Referred	0	0	0	0
Total	695	638	76	15

*This category includes responsive action taken on a complaint received from a prior reporting period.

DHS separate 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 screening at the border or at airports.¹⁵
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

¹⁴ See *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*.

¹⁵ This category excludes *Freedom of Information Act* and *Privacy Act* requests for access, which are reported annually in the Annual FOIA Report, and *Privacy Act* Amendment requests, which are reported annually in the DHS Privacy Office Annual Report to Congress.

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:

National Protection and Programs Directorate (NPPD)

Complaint: NPPD received a complaint from an employee whose PII was inadvertently attached to another individual's record in the Government Travel Card database, which prevented the employee from obtaining a Travel Card. The employee was unable to correct the issue with the bank directly since the employee's information did not match the bank's records.

Disposition: NPPD worked with the bank to correct the employee's information. The data error occurred when data fields were incorrectly merged during a data transfer between two banks. The complaint was resolved to the individual's satisfaction.

U.S. Customs and Border Protection (CBP)

Complaint: The CBP INFO Center received a complaint from a female traveler who expressed concern about her experience during processing at a Port of Entry. The complainant requested a female officer to process her as she was uncomfortable being processed by a male, after which she felt that the CBP officers responded by "raising their voices and acting unprofessionally." The complainant stated that a female officer assisted her quickly and she was allowed to enter the United States, but the entire process made her "very uncomfortable."

Disposition: CBP INFO Center reviewed this complaint and sent a letter to the woman to apologize for any rude or unprofessional behavior, and explained the standard protocol for processing travelers in primary and secondary screenings. The letter recommended that the complainant speak with a supervisor in the future if she feels she is treated unprofessionally by a CBP employee.

VI. CONCLUSION

As required by the *9/11 Commission Act*, this quarterly report summarizes the DHS Privacy Office's activities from June 1, 2012 – August 31, 2012. The DHS Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.