Department of Homeland Security

Privacy Office

Third Quarter Fiscal Year 2013 Report to Congress

August 2013

Homeland Security

I. FOREWORD

August 30, 2013

I am pleased to present the Department of Homeland Security Privacy Office's *Third Quarter Fiscal Year 2013 Report to Congress* for the period March 1 – May 31, 2013.[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 by DHS.

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

---

[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.

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 Privacy Office at 202-343-1717 or privacy@dhs.gov. More information about the Privacy Office, along with copies of prior reports, is available on the Web at: www.dhs.gov/privacy.

Sincerely,

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

DHS PRIVACY OFFICE
THIRD QUARTER FISCAL YEAR 2013
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 (Department or DHS) Privacy Office (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 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 Third Quarter Fiscal Year 2013	
Type of Review	**Number of Reviews**
Privacy Threshold Analyses	161
Privacy Impact Assessments	16
System of Records Notices and Associated Privacy Act Exemptions	9
Privacy Act (e)(3) Statements	12
Computer Matching Agreements	8
Data Mining Reports	1
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests	0
Other Privacy Reviews	0
Total Reviews	***208***

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 personally identifiable information (PII). As of May 31, 2013, 87 percent of the Department's *Federal Information Security Management Act* (FISMA) systems requiring a PIA had one in effect.

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

During the reporting period, the Office published 16 new, updated, or renewed PIAs, and 9 are summarized below. Published PIAs are available on the Privacy Office website, www.dhs.gov/privacy.

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

DHS/CBP/PIA-016 – U.S. Customs and Border Protection Form I-94 Automation *(March 1, 2013)*
Background: United States Customs and Border Protection (CBP) issues Form I-94 to provide documentation of the approved length of stay and departure of nonimmigrant aliens. The current form is paper-based and includes a detachable portion with an admission (I-94) number, which the nonimmigrant alien keeps while in the United States as documentation of status. CBP issued an interim final rule to enable CBP to transition from a paper Form I-94 to an automated process in certain circumstances.

Purpose: CBP conducted this PIA to address how it implements the electronic Form I-94 pursuant to the Fair Information Practice Principles (FIPPs).

DHS/USCG/PIA-019 – Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard *(March 25, 2013)*
Background: The United States Coast Guard (USCG) published a Notice of Proposed Rulemaking (NPRM) to require owners or operators of vessels and facilities that meet certain risk factors to use, as an access control measure, electronic readers that work in combination with the TWIC. The proposed rule requires owners or operators whose vessels or facilities meet a certain risk threshold to capture the following information when an individual's TWIC is scanned using a TWIC reader: (1) the TWIC-holder's Federal Agency Smart Credential-Number; (2) the date of scan; (3) the time of scan; and (4) only if captured, the name of the individual TWIC-holder. Identity verification is accomplished by matching one of the fingerprint templates stored in the TWIC to the TWIC-holder's live sample biometric using an electronic TWIC reader.

Purpose: USCG conducted this PIA because the proposed rule requires third parties (i.e., owners or operators of certain regulated vessels and facilities) to collect limited PII from TWIC readers.

DHS/OPS/PIA-004(e) – Publicly Available Social Media Monitoring and Situational Awareness Initiative Update *(April 1, 2013)*

Background: The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), leads the Publicly Available Social Media Monitoring and Situational Awareness Initiative to assist DHS and its components involved in fulfilling OPS statutory responsibility to provide situational awareness and establish a common operating picture for the Federal Government, and for state, local, and tribal governments, as appropriate. Under this initiative, OPS does not: (1) post any information on social media sites; (2) actively seek to connect with other individual social media users, whether internal or external to DHS; (3) accept invitations to connect from other individual social media users, whether internal or external to DHS; or (4) interact on social media sites. However, OPS is permitted to establish user names and passwords to form profiles and connect with operationally relevant government, media, and subject matter experts on social media sites (such as those listed in Appendix A) in order to use search tools under established criteria and search terms (such as those listed in Appendix B) for monitoring that supports providing situational awareness and establishing a common operating picture.

Purpose: After conducting the fourth Privacy Compliance Review (Media Monitoring Initiative) the Privacy office determined that this PIA should be updated to reflect changes recommended to and implemented by the NOC. These include improvements in tracking of searches conducted to identify relevant reports, incorporation of additional guidance into standard operating procedures (SOP) concerning the appropriate use of the NOC Media Monitoring Capability (MMC) Twitter profile, and clarification of language in the Analyst's Desktop Binder and SOPs to emphasize that information in NOC MMC reports must be operationally relevant to DHS in all cases. DHS replaced the 2011 published DHS/OPS/PIA-004(d) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update PIA with this PIA.

DHS/NPPD/PIA-027 – EINSTEIN 3 Accelerated (E3A) *(April 19, 2013)*

Background: DHS's Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS will deploy EINSTEIN 3 Accelerated (E3A) to enhance cybersecurity analysis, situational awareness, and security response. With E3A, DHS will not only be able to detect malicious traffic targeting Federal Government networks, but also prevent malicious traffic from harming those networks. This will be accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks.

Purpose: NPPD conducted this PIA because E3A includes the analysis of federal network traffic that may contain PII.

DHS/USCIS/PIA-006(b) – Systematic Alien Verification for Entitlements (SAVE) Program Update *(April 19, 2013)*
Background: United States Citizenship and Immigration Services' (USCIS) Verification Division published this update to the SAVE Program PIA. SAVE is a fee-based inter-governmental initiative designed to help federal, state, tribal, territorial and local government agencies confirm status prior to granting benefits and licenses, as well as for other lawful purposes.

Purpose: USCIS conducted this update to: 1) describe the expanded use of the Photo Matching Tool technology; and 2) introduce the implementation of the electronic form G-845, *Document Verification Request*.

DHS/FEMA/PIA-028 – Mapping Information Platform (MIP) *(April 30, 2013)*
Background: The Federal Emergency Management Agency's (FEMA) Federal Insurance and Mitigation Administration (FIMA) owns and operates the Mapping Information Platform (MIP). MIP supports the National Flood Insurance Program and provides an online method for property owners and certifiers to reference and petition to update the maps that define floodplains throughout the United States and its territories.

Purpose: FEMA conducted this PIA because the MIP collects, uses, maintains, retrieves, and disseminates the PII of (1) property owners seeking changes to FEMA flood maps or purchasing flood mapping services and products through MIP; (2) certifiers (i.e., Registered Professional Engineers and Licensed Land Surveyors) acting on behalf of property owners; and (3) state and local government officials with authority over a community's floodplain management activities. This PIA replaces the previously published DHS/FEMA/PIA-003.

DHS/ICE/PIA-035 – Imaged Documents and Exemplars Library (IDEAL) *(May 13, 2013)*
Background: The United States Immigration and Customs Enforcement (ICE) Homeland Security Investigations-Forensic Laboratory (HSI-FL) owns and operates the Imaged Documents and Exemplars Library (IDEAL), a centralized repository of images of and document characteristics from travel and identity documents, as well as reference materials concerning attempts to counterfeit or tamper with those documents. IDEAL is used to support the HSI-FL's mission to conduct forensic document analysis in support of law enforcement investigations and activities by DHS and other agencies. IDEAL assists HSI-FL employees in locating, verifying, and storing documents in the HSI-FL Library.

Purpose: ICE conducted this PIA because PII of individuals is often captured in the images and other records maintained in IDEAL.

DHS/OPS/PIA-008(b) – HSIN Release 3 User Accounts: Identity Proofing Service *(May 22, 2013)*
Background: The Homeland Security Information Network (HSIN) is maintained by OPS. HSIN facilitates the secure integration and interoperability of information sharing resources among federal, state, local, tribal, territorial, private-sector, commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities. The HSIN program prepared this PIA Update to clarify information about HSIN's use of and the data handling practices of the identity proofing service (IDP Service).

Purpose: OPS conducted this PIA to document the program's updated understanding of the information collected and stored by the IDP Service during, and following, new user registration on the HSIN R3 platform.

DHS/CBP/PIA-014 – Centralized Area Video Surveillance System *(May 24, 2013)*
Background: The Centralized Area Video Surveillance System (CAVSS), a system of cameras and separate microphones recording video and audio, respectively, furthers CBP's mission by collecting and maintaining video images and audio recordings of persons involved in any incidents or disturbances while seeking entry or admission into the United States at a designated port of entry, including secondary inspections.

Purpose: CBP conducted this PIA because CAVSS uses information technology to collect, maintain, and disseminate PII in the form of video and audio recordings.

B. System of Records Notices

As of May 31, 2013, 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 Office published 7 SORNs and 2 Notices of Proposed Rulemaking, and 6 are summarized below. All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act exemptions are available on the Privacy Office website, www.dhs.gov/privacy.

DHS/CBP-018 – Customs-Trade Partnership Against Terrorism System of Records
DHS established a new system of records titled, "Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP-018 Customs-Trade Partnership Against Terrorism System of Records" (C-TPAT). This system of records allows CBP to collect and maintain records about members of the trade community related to the C-TPAT program. Businesses accepted into the program agree to analyze, measure, monitor, report, and enhance their supply chains in exchange for greater security and facilitated processing offered by CBP. The program allows CBP to focus its resources on higher risk businesses, and thereby assists the agency in achieving its mission to secure the border and facilitate the movement of legitimate international trade. This new system of records collects and manages information, including PII, about prospective, ineligible, current, or former trade partners in C-TPAT, and other entities and individuals in their supply chains. (78 Fed. Reg. 15889, March 13, 2013.)

- ***DHS/CBP-018 – Customs-Trade Partnership Against Terrorism System of Records, Notice of Proposed Rulemaking for Privacy Act Exemptions***
  Concurrently with the C-TPAT SORN, DHS published a Notice of Proposed Rulemaking in which the Department proposed to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (78 Fed. Reg. 15889, March 13, 2013.)

DHS/ICE-014 – Homeland Security Investigations Forensic Laboratory System of Records
DHS established a new system of records titled, "Department of Homeland Security, U.S. Immigration and Customs Enforcement, DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records." This system of records allows ICE to collect and maintain records by the Homeland Security Investigations Forensic Laboratory (HSI-FL). To facilitate forensic examinations and for use in forensic document training, research, and analysis, the HSI-FL maintains case files, a case management system, an electronic library of travel and identity documents (Imaged Documents and Exemplars Library), and a hard copy library referred to as the HSI-FL Library. (78 Fed. Reg. 28867, May 16, 2013.)

- ***DHS/ICE-014 – Homeland Security Investigations Forensic Laboratory System of Records, Notice of Proposed Rulemaking for Privacy Act Exemptions***
  Concurrently with the HSI-FL SORN, DHS published a Notice of Proposed Rulemaking in which the Department proposed to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (78 Fed. Reg. 28761, May 16, 2013.)

DHS/CBP-007 – Border Crossing Information System of Records

CBP updated and reissued a current system of records titled, "Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP-007 Border Crossing Information System of Records." This system of records allows CBP to collect and maintain records on border crossing information for all individuals who enter, are admitted or paroled into, and—where available—exit from the United States, regardless of method or conveyance. CBP is updating this system of records notice to provide notice of the Beyond the Border (BTB) Entry/Exit Program with Canada. Through the Entry/Exit Program, the United States and Canada will exchange border crossing information about certain third-country nationals, permanent residents of Canada, and lawful permanent residents of the United States at all automated land border ports of entry. (78 Fed. Reg. 31958, May 28, 2013.)

- The exemptions for the existing system of records notice (73 Fed. Reg. 43457, July 25, 2008) will continue to apply for this updated system of records notice, and DHS will include this system in its inventory of record systems.

DHS/NPPD-001 – Arrival and Departure Information System (ADIS)

DHS updated and reissued a system of records titled "Department of Homeland Security/National Protection and Programs Directorate-001 Arrival and Departure Information System (ADIS) System of Records." This system of records allows DHS to collect and maintain records on individuals throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes. With the publication of this updated system of records, the following changes are being made: (1) a new category of records is being added; (2) the record source categories are being updated; and (3) administrative updates are being made globally to comply with the *Consolidated and Further Continuing Appropriations Act,2013*, which transfers the United States Visitor Indicator Technology (US-VISIT) program's biometric identity management functions to the Office of Biometric Identity Management (OBIM), a newly created office within the National Protection and Programs Directorate (NPPD).

This system of records notice updates the categories of records and record source categories. Originally, records could be derived from entry or exit data of foreign countries collected by foreign governments in support of their respective entry and exit processes. These records collected from foreign governments were required to relate to individuals who have an existing record in ADIS. This update clarifies that although records collected from foreign governments must relate to individuals who have entered or exited the United States, in some instances there may be no pre-existing ADIS record for those individuals.

- The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice, and this system will be continue to be included in DHS's inventory of record systems. (78 Fed. Reg. 31955, May 28, 2013.)

C. Privacy Compliance Reviews

The 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 or Memoranda of Agreement.

The Privacy Office conducted a PCR for the E-Verify Self Check Program's use of a third-party identity proofing service[15] and found that the program is in compliance with the privacy requirements stated in its PIA and SORN. The Office is planning to conduct similar reviews for other DHS programs that use a third-party for identity proofing. These reviews will extend into Fiscal Year 2014.

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

[15] For information about E-Verify Self Check see: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_everifyselfcheck.pdf.

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

40,744 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. The Executive Office of the President requested permission to customize our mandatory online privacy training course to train all 3,000 White House employees on best practices for safeguarding PII. They reviewed courses from many agencies and decided ours was the best fit for their needs.

New Employee Training

3,109 DHS personnel attended instructor-led privacy training courses, primarily privacy training for new employees:

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

Miscellaneous Training

- The Privacy Office provides privacy training to Reports Officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program.
    - During this reporting period, the Office trained 36 Reports Officers on privacy policy.

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

B. DHS Privacy Office Awareness & Outreach

Publications

The Privacy Office issued two major publications this quarter:

- *2013 Chief Freedom of Information Act (FOIA) Officer Report to the Attorney General of the United States*, summarizing the Department's accomplishments in achieving its strategic goals related to FOIA, transparency, and openness from March 2012 through March 2013; and

- *2012 Annual Freedom of Information Act Report to the Attorney General*, which highlights the unprecedented number of FOIA requests and appeals the Department received this fiscal year, and the sizable reduction of its backlog of requests and appeals.

Meetings & Events

- Unmanned Aircraft Systems (UAS) Senate Judiciary Staff Briefing – On March 19, the Privacy Office, in conjunction with CBP, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of Policy, briefed Senate Judiciary Committee staff on DHS's use of UAS.

- Meeting with Japanese Cabinet Secretariat Representatives – On March 25, the Privacy Office hosted four officials from Japan, including two representatives from the Cabinet Secretariat's Office for Social Security Reform. The Japanese Government is considering introducing a process equivalent to the PIA process and seeks to learn from DHS experience. Privacy Office staff provided an overview of the U.S. privacy framework, along with specific DHS privacy policies and practices, including compliance and oversight mechanisms.

- Public Outreach Meetings: Executive Order 13636 – On April 10, the Privacy Office and CRCL hosted the first in a series of biweekly overview presentations with the Integrated Task Force Working Group leads. The overviews detailed the ongoing work of departments and agencies in implementing cybersecurity and critical infrastructure protection efforts pursuant to Executive Order 13636 and Presidential Policy Directive 21. These meetings are expected to conclude in early June.

- Sixth Annual American Society of Access Professionals National Training Conference – On May 13, the Acting Chief Privacy Officer participated in two presentations: the *Ask the Experts on Privacy* panel, and the *Succession Planning* session; the Associate Director of Privacy Oversight was a presenter on the *Breaches and Remediation* panel.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency

- Continued to train all new headquarters employees and contractors by way of Enter-On-Duty orientations.
- Delivered specialized privacy awareness training to personnel at the Office of the Chief Component Human Capital Officer located at the Virginia National Processing Service Center in Winchester, Virginia, and the Distance Learning Branch/Emergency Management Institute located in Emmittsburg, Maryland.

National Protection and Programs Directorate

- Participated in a presentation titled *The 411 on Cybersecurity, Information Sharing and Privacy* in March 2013 at the International Association of Privacy Professionals Global Privacy Summit in Washington, D.C. NPPD's Senior Privacy Officer, along with privacy professionals from the Department of Health & Human Services and the Department of Commerce, provided an overview of the government's ongoing efforts to improve cybersecurity through information sharing, insights on the structures in place to help protect privacy, and a discussion of some major legal and policy issues that public- and private-sector players are facing as the cybersecurity landscape evolves.
- Provided training to field chemical inspectors on best practices for protecting PII, on March 12, 2013.
- Spoke to employees and their children about safe online practices on *Bring your Daughters and Sons to Work Day* in April 2013, in an effort to make kids aware of the dangers associated with disclosing personal information online.
- Co-hosted, along with CRCL, three training sessions on privacy, civil rights, and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products, in April and May 2013. This is part of a series of training events following NPPD's release of an external product checklist that will be used to help employees evaluate privacy, civil rights, and civil liberties concerns.
- Presented during a "brown bag" lunch training session for employees and contractors in the Office of Cybersecurity and Communications on May 16, 2013. The privacy briefing focused on identifying and protecting Sensitive PII, as well as incident handling procedures.
- Delivered role-based privacy training to the Federal Protective Service's Personnel Security Division, to include staff from each of the eleven regions, on May 22, 2013.
- Published the *Privacy Update*, NPPD's quarterly privacy awareness newsletter. This quarter's issue focused on the theme, "Cybersecurity Privacy," providing an overview of the privacy program's role in implementation of the president's Executive Order on Improving Critical Infrastructure Cybersecurity. This issue also provided employees with tips and best practices to protect against cyber attacks at home.

Office of Intelligence and Analysis

- Published an article in the quarterly staff newsletter on the increased risk of identity theft during tax season.

Transportation Security Administration

- Responded to 29 individuals seeking guidance about PII via the Transportation Security Administration (TSA) Privacy email box.
- Published an online telework brochure to promote best practices for safeguarding PII in remote locations.
- Presented information on Sensitive PII, and the role of the TSA Privacy Office to various employees.
- Reviewed 18 intelligence products for sensitive privacy information.

United States Citizenship and Immigration Services

- Issued a guidance memorandum on April 30, 2013, to inform employees and contractors of the release of the new online Privacy Awareness Training that focuses on privacy guidance as it pertains to USCIS-specific practices.
- Issued an updated guidance memorandum on March 14, 2013, to employees and contractors of the requirement to use Public Key Infrastructure encryption software, and to ensure that Sensitive PII collected and disseminated by USCIS personnel is protected both within and outside of the DHS firewall.
- Issued a guidance memorandum on privacy compliance requirements on April 1, 2013, to remind USCIS employees and contractors of their responsibility to work with the USCIS Office of Privacy prior to starting any new initiatives that involve the collection, use, or storage of PII and the requirement to complete compliance documentation.
- Issued a guidance memorandum on the Enterprise Collaboration Network (ECN) on April 23, 2013, to inform employees and contractors of the privacy compliance process and the security requirements for maintaining Sensitive PII on ECN sites.
- Published the USCIS Office of Privacy second quarter newsletter, which focused on reporting privacy incidents, in addition to other helpful privacy news, tips, and guidance for safeguarding PII.
- Published multiple privacy tips on the USCIS intranet, highlighting topics that focused on the appropriate use, access, sharing, and disposing of PII.
- Conducted and completed 14 site visits and risk assessments of various USCIS facilities to provide insight and recommendations to leadership on privacy risks, and how to improve privacy protections and awareness throughout each region.

United States Immigration and Customs Enforcement

- Moderated a discussion on best practices for handling privacy incidents at the *Incident Response Coffee Talk* sponsored by the CIO Council Privacy Committee, on April 23, 2013.
- Emailed tips on ways to secure and properly discard Sensitive PII to all employees on May 29, 2013.

V. PRIVACY COMPLAINTS AND DISPOSITIONS

For purposes of Section 803 reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with the DHS Privacy Office or DHS Components or programs. The categories of complaints reflected in the following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. U.S. citizens, Legal Permanent Residents, visitors, and aliens submit complaints.[17]

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

Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed, Responsive Action Taken	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	1	1	0	1
Redress	2	1	1	0
Operational	746	688	99	10
Referred	6	6	0	0
Total	***755***	***696***	***100***	***11***

.

DHS separates complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *Example*: An individual submits a complaint that alleges a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***Redress***: Issues concerning appropriate access and/or correction of PII, and appropriate redress of such issues.
    a. *Example*: Misidentifications during a credentialing process or during traveler inspection at the border or screening at airports.[18]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.
4. ***Referred****:* The DHS Component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another federal agency or entity, and referred the complaint to the appropriate organization. This category does not include internal referrals within DHS. The referral category both serves as a category of complaints and represents

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

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

   a. *Example*: An individual has a question about his or her driver's license or Social Security number, which the DHS Privacy Office refers to the proper agency.

DHS Components and the DHS Privacy Office report disposition of complaints in one of the two following categories:

1. *Closed, Responsive Action Taken*: The DHS Component or the DHS Privacy Office reviewed the complaint and took responsive action. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.

2. *In Progress*: The DHS Component or the DHS Privacy Office is reviewing the complaint to determine the appropriate action and/or response. This category identifies in-progress complaints from both the current and prior reporting periods.

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

United States Customs and Border Protection

Complaint: The CBP INFO Center was contacted by the complainant because she objected to the manner in which she was processed at a Port of Entry. The complainant reported that CBP officers emptied the contents of her purse in full view of other travelers, and asked her personal questions about her travel to the United States after she informed them that her identity was stolen, and before she was escorted to secondary.

***Disposition*:** The CBP INFO Center advised the complainant that it is standard procedure to verify the identity of individuals who have reported that their identity has been stolen. The CBP INFO Center explained that this verification process includes escorting the traveler to secondary examination, and asking personal questions to ensure the veracity of the individual's identity prior to admittance to the United States.

Complaint: The CBP INFO Center was contacted by the complainant concerning some difficulty she experienced retrieving her automated I-94 from the CBP website upon arrival in the United States. The complainant was referred to the Deferred Inspection Site at the airport where she entered the United States, but when her call to the Deferred Inspection Site went unanswered, she contacted the CBP INFO Center for further assistance.

***Disposition*:** The CBP INFO Center was able to view the complainant's I-94 in CBP's system, and walked her through the electronic I-94 process. As a result, she discovered that her passport number was incorrect in the CBP system. By using the number from an old expired passport, which she still had in her possession, the complainant and the CBP INFO Center were able to successfully view and print her I-94. The complainant was referred again to the Airport's Deferred Inspections to have her correct passport number recorded by CBP.

United States Immigration and Customs Enforcement

Complaint: A retired ICE employee submitted a complaint to the ICE Privacy Office alleging that a current ICE employee sent unencrypted emails containing Sensitive PII to his personal email account on three separate occasions. The emails contained retirement-related attachments that included Sensitive PII of the retiree and his wife. In addition to handling the complaint portion of the matter, the ICE Privacy Office also opened a privacy incident to address the fact that Sensitive PII was sent unencrypted outside of the DHS network.

***Disposition*:** To handle both the complaint and the incident, the ICE Privacy Office first reached out to the complainant to discuss his concerns. The ICE Privacy Office then contacted the current employee's supervisor to better understand the standard operating procedures for sending retirement-related documents to retirees. After discussing the matter with the ICE Privacy Office, the supervisor reminded all staff members of current procedures that describe how to properly protect documents. The complainant was notified in writing of the steps taken, and both the complaint and the privacy incident were closed.

VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from March 1 – May 31, 2013. The DHS Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.