Privacy Office

Second 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*

May 10, 2011

Homeland Security

I. FOREWORD

May 10, 2011

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Second Quarter Fiscal Year 2011 Report to Congress*. This quarterly report includes activities from December 1, 2010 – February 28, 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
SECOND QUARTER FY 2011
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. 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.

Q2 FY2011 Reviews	
Review Type	**# of Reviews**
Privacy Threshold Analyses	131
Privacy Impact Assessments	11
System of Records Notices and Associated Privacy Act Exemptions	4
Privacy Act (e)(3) Statements	6
Computer Matching Agreements	5
Data Mining Reports	1
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews for Q2 FY2011	***158***

Privacy Impact Assessments
At the Department, PIAs represent a substantial effort on the part of Components, Component Privacy Officers, Privacy Points of Contact, and the DHS Privacy Office. 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 February 28, 2011, 74 percent of the Department's FISMA systems that require a PIA are currently covered by a PIA. A complete list of PIAs conducted during this reporting period can be found on our website. Below are some examples:

- ***Advanced Imaging Technology Update*** – The Transportation Security Administration (TSA) has deployed Advanced Imaging Technologies (AIT), including backscatter x-ray and millimeter wave devices, for operational use to detect threat objects carried on persons entering airport sterile areas. In February 2011, TSA began testing, at three airports, Automatic Target Recognition software, which, when used on existing AIT machines, displays anomalies on a generic figure, as opposed to an image of a specific individual's body. Since the new software uses a generic image that provides greater privacy protections for the individual being screened, systems using the new software will not isolate the operator viewing the image from the individual being screened. Individuals will continue to be given the option of undergoing a physical screening as an alternative to AIT screening. A PIA on AIT was originally published in January 2008. (January 25, 2011)

- ***Electronic Discovery Software System (EDSS)*** – This system is owned by the Office of the Principal Legal Advisor (OPLA) within U.S. Immigration and Customs Enforcement (ICE). EDSS supports the collection and organization of paper and electronic documents for analysis, review, redaction, and production to meet litigation discovery requirements. ICE may also use the system to process agency records in response to Freedom of Information Act (FOIA) or Privacy Act (PA) requests. ICE conducted this PIA because EDSS collects, analyzes, and stores PII. (December 10, 2010)

- ***H1-B Cap Registration*** – The United States Citizenship and Immigration Services (USCIS) is proposing to amend its regulation governing petitions by U.S. employers seeking H-1B nonimmigrant worker status for aliens subject to annual numerical limitations or who may be exempt from numerical limitations by having earned a U.S. master's degree or a higher degree (also referred to as the "65,000 cap" and "20,000 cap" respectively, or the "cap" collectively). Under the proposed rule, USCIS would establish H-1B Cap Registration, a mandatory registration process, to streamline the administration of H-1B petitions filed by employers. USCIS conducted this PIA because the H-1B Cap Registration notice of proposed rulemaking proposes a change to USCIS' collection of PII. (January 28, 2011)

- ***National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative*** – The National Infrastructure Coordinating Center (NICC), within the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (IP), is publishing this PIA to reflect activities under its Suspicious Activity Reporting (SAR) Initiative. The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior related to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism. NICC is conducting this PIA because the SAR Initiative occasionally contains PII, and NICC will collect and contribute SAR Initiative data for reporting and evaluation proceedings**.** As discussed in last quarter's report, this PIA is part of the Department-wide process for systematizing

how DHS handles SAR, and specifically SAR that meets the National ISE-SAR Initiative Functional Standard 1.5 (December 29, 2010)

- ***Medical Credentials Management System*** – The DHS Office of Health Affairs (OHA) is instituting a centralized medical credentialing system for DHS employees who provide health care services as part of their job, or as part of the Components' mission, or incidental to their ongoing operations. The purpose of the program is to formalize a process for verifying DHS employee (applicant) qualifications, licensure information, and relevant health care provider data. In accordance with DHS Directive 248-01, Medical Quality Management, the Assistant Secretary for Health Affairs and Chief Medical Officer is responsible for developing a centralized management system for approving credentials for DHS employee medical care providers. The credentialing process will include the collection and maintenance of information related to professional education, state license number(s), national registry certification, board certification, training and other pertinent information related to medical care practices. OHA conducted this PIA because the medical credentials management system will collect and maintain PII on DHS medical care providers. (February 10, 2011)

System of Records Notices

In addition to the PIAs published during this reporting period, DHS also published four Privacy Act SORNs to support systems at USCIS, the Federal Emergency Management Agency (FEMA), ICE, and Operations. As of February 28, 2011, 94 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. Below are two examples of SORNs that were published during the reporting period and can be found on our website:

- ***DHS/USCIS-013, E-Verify Self Check System of Records*** – DHS/USCIS developed this SORN for records associated with E-Verify Self Check, a voluntary service available to any individual who wants to check his own work authorization status prior to employment, and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process. When an individual uses E-Verify Self Check, he will be notified either that: (1) his information matched the information contained in federal databases and he would be deemed work-authorized; or (2) his information was not matched to information contained in federal databases which would be considered a "mismatch." If the information was a mismatch, he will be given instructions on where and how to correct his record(s). On March 21, 2011, USCIS launched the first phase of the service to users who maintain an address and are physically located in Arizona, Idaho, Colorado, Mississippi, Virginia, or the District of Columbia. (February 16, 2011)

- ***DHS/FEMA-002, Quality Assurance Recording System of Records*** – This system will record telephone calls made or received by FEMA employees and/or contractors at FEMA's National Processing Service Centers. It will also record the screen activity in the National Emergency Management Information System for both call-related customer service transactions and case review transactions not related to a telephone call. This system of records may contain the PII of disaster assistance applicants, which is covered by DHS Federal Emergency Management Agency-008, Disaster Recovery Assistance Files System of Records, September 24, 2009, and will contain the PII of FEMA employees and/or contractors that provide customer service to them. The proposed system will be used for internal employee performance evaluations, training, and quality assurance purposes to improve customer service to disaster assistance applicants. This collection was previously covered by the DHS/All-020 Internal Affairs System of Records, November 18, 2008. (February 15, 2011)

Computer Matching Agreements

Pursuant to 5 U.S.C. § 552a(a)(8), a "matching program" means any computerized comparison of two or more automated systems, of which one must be federal, for the purpose of establishing the eligibility for cash or in-kind assistance or payments, or recovering debts, under federal benefit programs. The Department requires that Computer Matching Agreements be developed and then approved by the Department's Data Integrity Board for any matching program when there is a comparison of two systems of records that may result in identifying individuals who meet the statutory characteristics outlined above. No record which is contained in a system of records may be disclosed to a recipient agency or non-federal agency for use in a matching program except pursuant to a written Computer Matching Agreement between the source agency and the recipient agency or non-federal agency. These agreements are valid for 18 months, with the option of extending them for one additional year.

- ***USCIS Verification Division Systematic Alien Verification for Entitlement (SAVE) Program*** – During this reporting period, the DHS Privacy Office facilitated the review and approval of five extension Computer Matching Agreements between SAVE and the following agencies: California Department of Healthcare Services, Massachusetts Division of Unemployment Assistance, New Jersey Department of Labor and Workforce Development, New York Department of Labor, and the Texas Workforce Commission. SAVE assists federal, state, and local benefit-granting agencies with determining an alien applicant's immigration status. This helps to ensure that only entitled applicants receive public benefits and licenses, such as Social Security benefits, Medicare/Medicaid, and driver's licenses. Agencies which have been approved for the program may verify immigration status through Verification Division's internet portal, via a web services connection, or batch data transfer. The large majority of SAVE's 777 (and growing) participating agencies verify applicants' status using an internet portal or web services. However, several verify status using batch data transfers, thus requiring these agencies to sign a Computer Matching Agreement with the Department in compliance with the Privacy Act.

III. ADVICE AND RESPONSES

Privacy Training, Awareness and Outreach

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

- 3,280 DHS personnel attended instructor-led privacy training courses.
- 29,279 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. Component Privacy Offices may 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 for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to over 100 staff from 4 fusion centers.
- The DHS Privacy Office also continued to provide training to intelligence professionals selected for assignment to fusion centers from I&A, as required under section 511 of the *9/l1 Commission Act*.

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, or by clicking on the links below.

- *Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests*, (February 2011). Department policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended.
- *OIG Privacy Incident Report and Assessment*, (February 2011). The Chief Privacy Officer issued a public report on a privacy incident involving the Office of Inspector General (OIG) and contractor KPMG. The report makes findings and recommendations addressing compliance with privacy policies and recommends steps for prevention and mitigation of similar privacy incidents.
- *2010 Data Mining Report*, (December 2010). This report describes DHS programs, both operational and in development, that involve data mining as defined by the *Federal Agency Data Mining Reporting Act of 2007*. The report provides the detailed information required by the Act and includes updates on program modifications and other developments since the Department issued its 2009 Data Mining Report in December 2009.
- *FOIA Annual Report for 2010*, (February 2011). Annual report to the U.S. Attorney General.

- *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.)
- *OECD Privacy Guidelines: Thirty Years in the Public Sector* (December 3, 2010). This report by The Privacy Projects was partially funded by the DHS Privacy Office and is intended to inform the OECD in its review of whether to revise the OECD privacy guidelines.

Meetings & Events

- American Society of Access Professionals (ASAP) - On December 1, 2010, the Associate Director for FOIA Policy and Program Development presented *Dealing with a Drain on FOIA Resources* at the American Society of Access Professionals in Washington, D.C..
- The Constitution Project – On December 7, 2010, the Chief Privacy Officer participated in a panel discussion hosted by The Constitution Project. The panel followed the release of The Constitution Project's report entitled, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*.
- U.S. – European Union (EU) Passenger Name Record (PNR) Agreement – On December 8, 2010, the Chief Privacy Officer and the International Privacy Policy (IPP) Director participated in a National Targeting Center briefing and tour for the Hungarian Minister of the Interior and the U.S. Ambassador to the EU. The briefing and tour were intended to give the participants greater insight into DHS policies and practices in preparation for renegotiation of the 2007 U.S. – EU PNR Agreement.
- Office of the General Counsel (OGC) Intelligence and National Security Law Conference – On December 15, 2010, the Chief Privacy Officer participated in a panel entitled *Moving Forward: DHS's Response to the 12/25 Attempted Bombing*, as part of the Fifth Annual OGC Intelligence and National Security Law Conference.
- Privacy Information for Advocates – On December 17, 2010, the Chief Privacy Officer hosted the quarterly Privacy Information for Advocates meeting, which is designed to proactively engage the privacy community on privacy issues.
- Deputy Chief Privacy Officer (DCPO) Travel to Europe – The DCPO travelled to Belgium and Hungary the week of January 24, 2011 for initial discussion on the U.S. – European Union (EU) umbrella data protection agreement. DCPO also attended the U.S. – EU Justice and Home Affairs Ministerial, and presented at the European Data Protection Conference.
- RSA Conference – On February 15, 2011, the Chief Privacy Officer participated in a panel at the RSA Conference: *Security and Privacy for Open Government: Friends or Foes?*

B. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency Privacy Office
Provided privacy training to one of its National Processing Service Center (NPSC); to date, staff in all three of its regional centers have received privacy training. These centers handle a high percentage of sensitive PII submitted by disaster survivors seeking assistance.

Federal Law Enforcement Training Center Privacy Office
Sponsored a symposium on February 8-9, 2011, to assist in the development of DHS training for employees posted internationally. The DHS Privacy Office supports the Federal Law Enforcement Training Center 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.

Transportation Security Administration Privacy Office
- Placed a statement on the earnings and leave statements of all employees to raise awareness of the importance of safeguarding sensitive PII.
- 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.
- Reviewed 18 intelligence products for sensitive PII.
- Attended one outreach meeting with the American Civil Liberties Union.

U.S. Citizenship and Immigration Services Privacy Office
- Participated in a privacy and security breach incident training exercise at the Security Network Operations Center (SNOC) in Broomfield, CO. During the two-day "mock training event", personnel were presented with a fictitious data security incident in which they had to assess the nature and circumstances, devise and coordinate a response, and implement appropriate remediation and mitigation actions. The Privacy Officer's role was to advise and recommend courses of action. In addition, a site visit to the Denver District Office was conducted along with a leadership briefing and privacy awareness training for nearly 100 employees and contractors.
- Amended the Privacy Incident Response Plan to include an appendix, *Breach Notification Procedures for Confirmed Privacy Incidents.*

U.S. Coast Guard Privacy Office
Held a one-day Privacy Act training session in December 2010 on the DHS privacy compliance management process was provided to 13 Coast Guard personnel from the Office of Project Development at Coast Guard headquarters.

U.S. Immigration & Customs Enforcement Privacy Office
Launched a new, mandatory privacy training module for all personnel entitled, *Privacy Training for SharePoint Collaboration Site Users*, that raises employee awareness about the posting of sensitive PII on SharePoint collaboration websites.

IV. 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 and lawful permanent residents as well as visitors and 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	5	5	0	0
Redress	6	7	0	2
Operational	149	132	21	8
Referred	4	9	0	1
Total	***164***	***153***	***21***	***11***

*This category may include responsive action taken on a complaint received from a prior reporting period.
**This category reflects an additional referred complaint that was not accounted for in a prior reporting period.

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.
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.
   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.

[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.

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

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
Following media reports that TSA would implement new pat-down procedures, TSA received complaints from several individuals who were upset by their experience. TSA understands that while passengers may differ in their level of comfort with the pat-down, all travelers should expect to be treated professionally by the TSA workforce. TSA works with a variety of groups to determine appropriate methods to address public concerns, and to implement appropriate training. Given the ongoing threat to airline passenger safety, passengers should continue to expect that TSA will employ a wide variety of security measures.

U.S. Visitor and Immigrant Status Indicator Technology
During this reporting period, U.S. Visitor and Immigrant Status Indicator Technology **(**US-VISIT) received a redress request pertaining to a biometrics issue. An individual complained that he had experienced delays during his last few entries into the United States, causing him a lot of inconvenience. US-VISIT reviewed his record and determined that the problem was due to incorrectly labeled finger prints at the port of entry during one of his visits. This caused the prints that were taken on subsequent entries to mismatch against the prints on file. US-VISIT was able to correct his record.