

DHS Data Privacy and Integrity Advisory Committee
Summary of Public Meeting
September 28, 2010, Washington, DC

Committee members in attendance:

Richard V. Purcell, Chairman	David A. Hoffman
Ana I. Anton	Lance Hoffman
Ramon Barquin	Joanne McNabb
Daniel W. Caprio Jr.	Charles Palmer
Renard Francois	Neville Pattinson
James W. Harper	John Sabo
Kirk Herath	Lisa J. Sotto

Also in attendance:

Mary Ellen Callahan, Chief Privacy Officer and Sponsor
Martha K. Landesberg, Executive Director and Designated Federal Official

Chairman Richard Purcell called the meeting to order at 8:40 a.m.

DHS Privacy Officer's Update:

Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security (DHS)

Ms. Callahan gave a brief overview of the meeting agenda and announced the hiring of two new component privacy officers in the National Protection and Program Directorate (NPPD) and the Office of Intelligence and Analysis (I&A), respectively. With these new additions, all DHS operational components other than the Science & Technology Directorate (S&T) have privacy officers on board; and S&T is in the final stages of selecting its privacy officer.

Ms. Callahan then provided an update on the activities of the DHS Privacy Office since the Committee last met on May 28, 2010, including accomplishments by the Freedom of Information Act, Policy, Compliance, Technology and Intelligence, Incident and Inquiries, and International Privacy Policy groups.

The FOIA Group

- By the end of August 2010, received 120,000 FOIA requests for Fiscal Year (FY) 2010. U.S. Citizenship and Immigration Service (USCIS) alone received over 10,000 FOIA requests in August.
- Made substantial continued progress in reducing the Department's backlog of FOIA requests; the Department is likely to meet the stated goal of reducing its backlog by 15%.
- Completed two compliance milestones: the draft FOIA/Privacy Act System of Record Notice (SORN) that was published in October 2009 became final in August; also in August, the Chief Privacy Officer signed a DHS-wide Privacy Impact Assessment (PIA) covering all systems used to collect data for processing FOIA requests.

Policy Group

- Released the 2010 DHS Privacy Office Annual Report to Congress on September 17th.
- Published a *Guide to Implementing Privacy*, which describes how the Privacy Office carries out its duties and responsibilities and how the office works to promote a privacy culture at DHS.
- Debra Diener joined the Privacy Office as Senior Advisor and Director of Privacy Policy in September.

Compliance Group

DHS Data Privacy and Integrity Advisory Committee
Minutes – Public Meeting – September 28, 2010

- Approved 202 Privacy Threshold Analyses (PTAs), 20 PIAs, and three SORNs since the May 2010 DPIAC Meeting.
- Reviewed the privacy documentation for 91 major IT investment systems and failed 11 of those systems for lack of privacy compliance documentation. The Privacy Office is working with the systems that failed to improve their privacy practices and documentation.
- Increased the Department's Federal Information Security Management Act (FISMA) scores. The Department is continuing to work with components that need to improve their scores.
- Published the first Privacy Compliance Review, which covered the Department's use of social media for situational awareness during the Winter Olympics and after the earthquake in Haiti.
- Working to systematize how the Privacy Office reviews ongoing programs for compliance with DHS policies, procedures, and public statements.

Privacy Technology and Intelligence Group

- Participated in the efforts of cybersecurity committees internal and external to the Department.
- Working collaboratively with S&T to develop an "enterprise" approach to privacy compliance across S&T programs.

Incidents and Inquiries

- Held the third Privacy Incident Handling Quarterly Meeting on June 29, 2010 to discuss privacy incidents at DHS that took place between February and May 2010.
- Held the second annual privacy incident management meeting of the DHS Core Management Group on September 14, 2010, to discuss the root causes of incidents and to provide targeted training to lessen the likelihood of incidents in the future.

Privacy Office Communications

- Developed an external communication plan to raise public awareness of the Office's work in both the privacy community and the general public. This includes: leveraging the www.dhs.gov/privacy website to ensure the public is aware of PIAs, SORNs, public events, reports, and other publications; email campaigns to constituents; and occasional articles in the DHS Blog presenting the Chief Privacy Officer's thoughts on privacy topics of public interest.

Federal Chief Information Officer (CIO) Council

- The Chief Privacy Officer serves as Co-Chair of the CIO Council's Privacy Committee.
- The Deputy Chief Privacy Officer co-chairs the Privacy Committee's International subcommittee, which is collaborating on an article for European audiences on how the U.S. uses compliance documentation to increase accountability. The Subcommittee is also developing an International Privacy Laws Matrix for use in international negotiations.
- The Privacy Office's Associate Director for Policy co-chairs the Privacy Committee's Best Practices subcommittee, which led the drafting of the Privacy Committee's *Elements of a Federal Privacy Program*, a comprehensive guide to building an effective agency privacy program, issued June 2010.

I&A Product Reviews

- Privacy Office staff reviewed approximately 80 analytic products and 200 Homeland Intelligence Reports prepared by I&A analysts.

Fusion Centers

- Together with the DHS Office for Civil Rights and Civil Liberties, the Privacy Office completed its train-the-trainers sessions for state and local fusion center privacy offices. These sessions, held at regional fusion center conferences, trained fusion center privacy officers in techniques they can use to provide

privacy training for their own staff. Privacy officers of 69 of the 72 fusion centers attended these sessions.

- Provided in-person training, together with CRCL, to seven centers in two states.
- Continue to review fusion center privacy policies to confirm that they are at least as comprehensive as the federal privacy guidelines for the Information Sharing Environment; and continued to provide ongoing support for fusion centers as they create privacy policies.

Privacy Training within DHS

- The Associate Director for Communications and Training worked intensively to enhance the Department's privacy curriculum by launching new versions of the online "Culture of Privacy Awareness" course, the introduction to DHS privacy policy and FOIA that all new employees receive as part of their initial DHS orientation, and the privacy compliance portion of DHS 101, the Department's comprehensive course on DHS operations that is open to all employees.

International Privacy Policy Group

- Coordinated with the DHS Office of General Counsel and Office of International Affairs, and the Departments of State and Justice, on current privacy issues related to U.S.-European Union (E.U.) information sharing arrangements, on a binding U.S.-E.U. agreement based on the High Level Contact Group principles, and on redress options for non-U.S. persons.
- Regularly participate in U.S. interagency and multilateral planning meetings of the Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy.
- Met with training and international staff at DHS to determine the best means of delivering Privacy training to DHS international liaisons and attaches. Currently working on online training options and hard copy "take aways," and discussing how best to incorporate this material into existing U.S.-based training programs.
- Continue to promote DHS privacy compliance practices to myriad international officials and other international audiences to increase transparency and promote privacy best practices.

Presentation on DHS Privacy Compliance Reviews: Building Accountability

Jamie Pressman, Associate Director of Privacy Compliance, DHS Privacy Office

Ms. Pressman briefed the Committee on the Privacy Office's efforts to build more accountability into the DHS Privacy Compliance process through compliance reviews. The Privacy Office works with the DHS CIO to incorporate privacy requirements into processes for IT system and program development, budget, rulemaking, and the Paperwork Reduction Act. The Privacy Office has a unique position as both an advisor and an oversight body for the Department's privacy sensitive systems and programs. Ms. Pressman discussed the new privacy compliance review process, which allows the Privacy Office to initiate reviews at the discretion of the Chief Privacy Officer, as well as when an agreement obligates the Privacy Office to conduct a review of a program or system to assess compliance. A Memorandum of Understanding (MOU) with an external entity that involves information sharing may have a provision for DHS to review use of the information. Ms. Pressman described a review conducted on the Department's use of social media as well as the Compliance Group's work with the Office of Operations Coordination and Planning (OPS). OPS prepared a PIA to describe their planned use of social media for monitoring the 2010 Winter Olympics and the earthquake in Haiti. Compliance reviews will be published on the Privacy Office's website.

Ms. Pressman explained the eight basic steps in a privacy compliance review:

1. Collecting and reviewing available background information on the program or system in question.
2. Formulating the review objectives, which typically includes assessing a program's compliance with its current privacy documentation and applicable DHS policies.
3. Notifying the program that the Privacy Office is going to conduct a review.

4. Formulating the review questions and document requests.
5. Interviewing program staff.
6. Analyzing the documentation and interviews and documenting preliminary conclusions.
7. Drafting a report of findings and recommendations and meeting with the program to discuss them; and
8. Issuing a final report and posting it on the Privacy Office website. Ms. Pressman then addressed questions from the Committee.

Presentation on Privacy Training in DHS

Steve Richards, Associate Director of Communications and Training, DHS Privacy Office

Mr. Richards' mission is to increase privacy awareness across the Department and to strengthen the Office's communications both within DHS and with the public. It is important for every DHS employee to know the privacy risk management framework, the Fair Information Practice Principles (FIPPs), and the privacy compliance process. Mr. Richards described the learning tools he has developed, including a Safeguarding Personally Identifiable Information (PII) Fact Sheet. Mr. Richards stressed that ongoing privacy education is required for every DHS employee. The *Culture of Privacy Awareness* course is being updated, as have been the privacy modules of DHS 101 and the DHS new hire training. USCIS and U.S. Immigration and Customs Enforcement (ICE) conducted job-specific privacy training this year to guide people on handling sensitive PII, and Mr. Richards seeks to leverage training across the other DHS components.

Mr. Richards serves as an advisor to the component privacy officers and the Privacy Points of Contact, to help them implement privacy best practices. Half of the components have conducted activities to increase privacy awareness, such as a Privacy Week. Ten of the twelve components have developed either an intranet or an extranet on DHS.gov, complete with privacy resources. In addition to his other training responsibilities, Mr. Richards worked with the Office of Civil Rights and Civil Liberties (CRCL) to provide the train-the-trainers course to state and local fusion center privacy offices.

Mr. Richards is also responsible for improving the Privacy Office's website, which he has developed as a "task-based" site where people can quickly find what they are looking for, such as FOIA requests, PIAs, and SORNs. Mr. Richards also manages the Privacy Office's new e-mail campaign strategy that includes sending regular messages to 300 constituents in the public to help position the Office as a thought leader in the privacy field. Mr. Richards concluded his presentation by detailing the Kirkpatrick model, which is a training metrics model used to measure success in FY 2011 that he will implement across the Department. He then took questions from Committee members.

Presentation on Customs and Border Protection (CBP) Implementation of DHS Privacy Policy

Laurence E. Castelli, Privacy Officer, CBP

As privacy officer, Mr. Castelli is responsible for monitoring CBP's compliance with all federal privacy laws and regulations, for implementing corrective, remedial or preventative actions, and for notifying the DHS Privacy Office of issues of non-compliance when necessary. Mr. Castelli and his staff approach privacy in two ways: by operationalizing privacy and by implementing and embedding privacy compliance into the culture of CBP. Mr. Castelli began his work as privacy officer by revisiting old CBP SORNs and looked at staffing issues to better implementing privacy. The CBP Privacy Office meets with the Office of Information Technology to discuss integrating privacy compliance into new IT developments. Mr. Castelli restructured the old Treasury Enforcement Communications Systems (TECS) SORN into five different SORNs. The purpose of this restructuring was to allow the public to better understand the different types of information that CBP collects at the border and how that information is collected. Within the CBP Privacy Office Mr. Castelli has created two different practice groups, privacy compliance and information sharing, to better integrate privacy into CBP's operations.

Mr. Castelli concluded his presentation by discussing privacy training within CBP. Mr. Castelli is working with the Privacy Office's Associate Director of Communications and Training to create more online training for CBP's Virtual Learning Center, an internal IT space for online training. CBP has two principal training courses that every employee is required to take before accessing administrative systems. The general Privacy Awareness course and the TECS Privacy Awareness course are required annually as a way of reinforcing privacy concepts. Mr. Castelli responded to questions and comments from the Committee following his presentation.

Public Comments and Questions to the Committee

Chairman Purcell opened the floor for public comments at 11:58 a.m. As there were no public comments, Chairman Purcell adjourned the meeting.

The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of DHS and the Chief Privacy Officer of DHS on programmatic, policy, operational, administrative, and technological issues within the DHS that to training, protecting PII, the compliance review process, and imbedding privacy compliance. Materials presented to the Committee, including all Committee reports and recommendations, and meeting summaries and transcripts, are available to the public on the Committee's web page on the DHS Privacy Office website, www.dhs.gov/privacy.