

**DHS Data Privacy and Integrity Advisory Committee
Public Meeting
December 6, 2011**

Committee members in attendance:

Richard V. Purcell, Chairman		
Ramon Barquin	Lance Hoffman	Jules Polonetsky
J. Howard Beales III	Joanne McNabb*	John Sabo
A. Michael Froomkin*	Greg Nojeim	Lisa Sotto
Joanna L. Grama*	Charles Palmer	Barry Steinhardt
David A. Hoffman	Christopher Pierson	

**By phone*

Also in attendance:

Mary Ellen Callahan, Chief Privacy Officer and Sponsor
Arthur Sepeta, Privacy Officer and Deputy Chief of the Information Compliance Branch, DHS
Office of Intelligence and Analysis
Donald Triner, Director of Ops Coordination, DHS Office of Operations Coordination and
Planning
Martha Landesberg, Executive Director and Designated Federal Official

Chairman Richard Purcell called the meeting to order at 1:10 pm.

DHS Privacy Officer's Update:

Ms. Callahan updated members on DHS Privacy Office activities that have occurred since their last meeting on October 5, 2011, including accomplishments of the Policy, Privacy Information Sharing and Intelligence, International Privacy Policy, Compliance, Privacy Technology, FOIA, and Incidents and Inquiries groups.

Policy

The Privacy Office has created a new internal online training resource center that will serve as a single source for DHS employees to access foundational skills in privacy and FOIA. The resource center points to a variety of classroom and online resources that can be used to further core competencies and technical skills.

Substantial progress has been made on the Privacy Office's privacy training course for DHS employees. Ms. Callahan will review the first complete draft of the course during the week of December 12.

The Privacy Office recently submitted its Fourth Quarter Section 803 Report to Congress. The report covers June 1, 2011, through August 31, 2011. The Office is also working to complete the

Department's 2011 Data Mining Report as required by the Federal Agency Data Mining Reporting Act. The report is scheduled to go to Congress by the end of the year.

In September, Ms. Callahan and Jonathan Cantor, the Department of Commerce Privacy and Open Government Officer, were elected to two-year appointments as Co-chairs of the Federal Chief Information Officer Council's Privacy Committee. This is Ms. Callahan's second term as Co-chair.

Martha Landesberg, the Privacy Office's Associate Director for Privacy, continues to co-chair the Privacy Committee's Best Practices Subcommittee, along with Roanne Shaddox from the Federal Deposit Insurance Corporation. In recent months, the subcommittee has focused on a Draft Privacy Controls Appendix to NIST Special Publication 800-53, which will for the first time integrate privacy standards into NIST's core security standards document. After the Subcommittee and NIST adjudicate public comments on the draft, a subsequent revision is expected to be released in January for additional public comment.

Privacy, Information Sharing, and Intelligence

Prior to the Committee's meeting in October, the Government Accountability Office (GAO) issued a report entitled *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*.

The report recommended that the Privacy Office explore new ways to ensure executive oversight of sensitive systems that, for national security reasons, are not appropriate for a public Privacy Impact Assessment (PIA). It also recommended that the Privacy Office review the Law Enforcement Information Sharing Program associated with Immigration and Customs Enforcement's (ICE) Pattern Analysis and Information Collection program (ICEPIC). While the Department disagreed with the GAO's definition of data mining, given that it was not the statutory definition, the Privacy Office has taken steps to review and implement the report's recommendations.

Ms. Callahan also briefed the staff of two Congressional committees about the steps the Privacy Office has implemented to ensure stronger and more robust privacy protections and to reduce the likelihood that such compliance gaps will exist in the future. These steps include: placement of component privacy officers in all operational components, mandatory periodic compliance updates, written Privacy Threshold Analyses (PTAs) to formally memorialize the decision-making process, a defined process for privacy protections, and a robust Privacy Office database to better track these developments.

DHS Information Sharing and Safeguarding Governance Board

On October 5, 2011, the DHS Information Sharing Governance Board (ISGB), the Executive-level steering committee and policy making body for information sharing in the Department, adopted a new charter under which the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties (CRCL), formerly ex officio members, are now full voting members. The new charter also incorporated additional security-related activities leading to the entity's name

being changed to the Information Sharing and Safeguarding Governance Board (ISSGB). The DHS Chief Information Officer currently serves as Vice Chair of the ISSGB.

State and Major Urban Area Fusion Centers

The Privacy Office trained a new DHS intelligence professional, now assigned to a fusion center, and provided training in two sessions to fusion centers serving the Commonwealth of Virginia, the Northern Virginia Regional Intelligence Center in Arlington, and the Virginia Fusion Center in Richmond. The next training session is planned for Colorado in January 2012.

International Privacy Policy

On November 17, 2011, Deputy Secretary of Homeland Security and lead negotiator for the United States Government Jane Holl Lute initialed an agreement between the United States and the European Union on the transfer and future sharing of Passenger Name Records (PNR). The Deputy Secretary's statement about the agreement is posted on the Department's website.

The Department continues to participate in interagency negotiating sessions for a US-EU "umbrella" agreement that would provide a framework for mutual recognition of privacy systems to facilitate the exchange of law enforcement information.

The European Commission recently announced Union-wide standards for the use of electromagnetic Advanced Imaging Technology (AIT). The Commission adopted the Transportation Security Administration's (TSA) privacy protections wholesale, including remote viewing, an inability to retain the images, and providing choice, as well as TSA's standards for systems utilizing the Automated Targeting Recognition platform. The Commission recommended not using AIT machines that use X-ray technologies to identify non-metallic threats for screening.

The Privacy Office is working closely with the Office of International Affairs and DHS components to ensure implementation of privacy protections in initiatives resulting from the February 2011 *US-Canada Beyond the Border Declaration* on perimeter security and economic competitiveness announced by the President and Prime Minister.

The Department also continues to ensure privacy law and policy, including DHS Information Sharing and Access Agreement (ISAA) requirements, is applied to other international initiatives. Recently, the Privacy Office's focus has been on information sharing that occurs under the auspices of the Five Country Conference (FCC), the expansion of Customs and Border Protection's (CBP) Global Entry Program, and Customs Mutual Assistance Agreements.

Privacy Office staff met with delegations from the German Ministry of Justice, the Canada Border Services Agency, and with Japanese academics. The meetings are part of the effort to better inform international partners about the U.S. privacy framework, DHS compliance and FOIA programs, and DHS privacy policy and best practices.

In November, Ms. Callahan attended the International Conference of Data Protection and Privacy Commissioners in Mexico City and presented on two panels: “Privacy by Design in the Public Sector” and “Data Protection Agency Oversight of Privacy at Law Enforcement Agencies.” IPP Director Lauren Saadat also presented on a panel on “Balancing Privacy and Recovery in a Natural Disaster,” which led to the Privacy Office being asked to serve on an advisory board for a project to inform EU policy on the use of social networks in disaster response.

Compliance

Over the past year several Privacy Office compliance analysts have accepted positions in privacy offices within the Department’s components, including Citizenship and Immigration Services (USCIS), Secret Service, and the United States Visitor and Immigrant Status Indicator Technology program (US-VISIT). Recently, the Privacy Office’s former Associate Director for Privacy Compliance, Eric Leckey, joined Federal Emergency Management Agency (FEMA) as its Privacy Officer. These staffing changes have provided excellent growth opportunities for DHS compliance professionals while benefiting the Department as whole.

By the end of FY 2011, DHS hit its 80 percent target FISMA score for PIAs. The Compliance team is working to raise its PIA score to 90 percent by the end of FY 2012. Since the last Committee meeting, the Compliance team has reviewed and approved 64 PTAs, 6 PIAs, 6 Privacy Act System of Records Notices, and 1 Computer Matching Agreement.

As the Privacy Office’s compliance process matures and scores improve, the Office has been working on ramping up its Privacy Compliance Review (PCR) capability. In addition to a PCR for ICEPIC LEIS, the Privacy Office recently initiated a PCR of the DHS Information Sharing Environment Suspicious Activity Reporting Initiative (a review that was built into this program’s design from the outset) and a combined PCR of EINSTEIN 2 and the Initiative 3 Exercise (from which the Office will draw recommendations for EINSTEIN 3). The Office also published its third PCR, a review of the Department’s National Operations Center Media Monitoring Capability. The Privacy Office plans to complete a PCR on US-VISIT in early 2012.

Privacy Technology

The Privacy Office’s Technology team continues to work closely with the National Protection and Programs Directorate (NPPD) Privacy Office on the EINSTEIN program, and is working on the PIA for the EINSTEIN 3 system.

The Privacy Office continues to host a speaker series that brings in experts to talk about emerging privacy issues. The series is now open to all federal workers – employees and contractors – and approximately 100 people attend each event. The next session will be on January 11, 2012, when representatives of the DHS Office of Cybersecurity and Communications will discuss the federal government’s cybersecurity program.

Freedom of Information Act

At the request of the House Committee on Government Oversight and Reform, on September 26, 2012, the GAO initiated a new multi-agency engagement pertaining to the Freedom of Information Act (FOIA). DHS and the Departments of Defense, Health and Human Services, and Justice—the Federal agencies with the largest FOIA caseloads—were selected to participate in the study. The study focuses on: 1) what agencies have done to assess and improve their FOIA programs since the Attorney General issued his FOIA guidelines in 2009 and 2) how agencies are complying with the requirement to make frequently-requested records available to the public electronically. The Privacy Office is the DHS lead for the study, but components that handle large volumes of FOIA requests, such as ICE and USCIS, have been consulted directly.

The FOIA team is supporting DHS' enterprise wide implementation of FOIA Xpress, an internet-based case tracking and reporting system specifically tailored for processing FOIA and Privacy Act Requests. The first phase, which will begin in January 2012, involves installing FOIA Xpress in pilot production in the Privacy Office for 15 users, then promulgating existing licenses to other DHS Headquarters components and eventually to other DHS components. The phased approach will take several months.

On November 22nd, the FOIA team, in collaboration with the Department of Justice, hosted training for DHS components on two often-used FOIA exemptions. Exemption (b)(5) addresses “inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency.” Exemption (b)(6) deals with the protection of law enforcement records or information. Approximately 70 DHS FOIA processors attended the training. The Privacy Office will continue providing similar training throughout the year to help senior FOIA processors develop expertise on the exemptions.

Incidents and Inquiries

On November 16, 2011, the Privacy Incidents and Inquiries team forwarded for Departmental clearance the revised Privacy Incident Handling Guidance (PIHG). The revision was prepared in close collaboration with the Chief Information Officer, the Chief Information Security Officer, the Chief Security Officer, component Privacy Officers/Privacy Points of Contact, and the Information Systems Security Managers. The revised and streamlined PIHG includes guidance for all stages of privacy incident handling, including reporting, escalation, investigation, mitigation, notification, and closure. This version contains more relevant examples and accurately represents the process as it exists today. The revision should be published by December 31, 2011, and will be posted on the DHS Privacy Office website.

In December 2011, Ms. Callahan will issue her second public report using her investigative authority. The report will provide findings and recommendations to address compliance with privacy policies at the component level that were examined during the course of the investigation. The report will be provided to DPIAC.

Ms. Callahan thanked the two sub-committees for their work on the policy and technology papers before responding to questions about the PNR agreement and utility of the policy and technology reports.

Update on the DHS Office of Intelligence & Analysis' Implementation of DHS Privacy Policy:

Arthur Sepeta, the Privacy Officer and Deputy Chief of the Information Compliance Branch in DHS's Office of Intelligence and Analysis (I&A) provided a historical perspective on his office and the intelligence community in general, addressing how and why the current I&A structure was created. The Homeland Security Act of 2002 established an Under Secretary to lead the Directorate of Information Analysis and Infrastructure Protection. Subsequent legislation and Executive Orders split the functions of Information Analysis and Infrastructure Protection into today's structure: the Office of Intelligence and Analysis, which is now part of the U.S. Government's Intelligence Community; and Infrastructure Protection, which is now part of DHS's National Protection and Programs Directorate.

Next, Mr. Sepeta discussed I&A information sharing related activities. Information sharing is an important aspect of identifying and tracking terrorists; however, in his role as the Privacy Officer at I&A, Mr. Sepeta also works to ensure privacy and civil liberties are protected. He also described the structure of I&A and the intelligence enterprise at DHS, which consists of FEMA, ICE, CBP, USCIS, United States Coast Guard, USSS, and TSA. I&A prepares intelligence products daily that are reviewed by CRCL, the Office of General Counsel, and the Privacy Office prior to release.

After his formal presentation, Mr. Sepeta responded to questions about the intelligence product review cycle, his role as I&A's Privacy Officer, and how I&A works with Fusion Centers.

Subcommittee Reports/Committee Discussion:

The Committee's Policy and Technology Subcommittee Chairs presented to the Committee draft reports including recommendations to the Department on federated information-sharing systems. Copies of the draft reports are available on the DPIAC website.

Policy Subcommittee

Lisa Sotto, Chair of the Policy Subcommittee summarized her Subcommittee's draft report, noting that it addressed access control, use of database control, applicable privacy policies, data integrity and quality assurance, accountability and audit procedures, data security, and redress. Two footnotes were added to the report as a result of discussions during the last Committee meeting. The first footnote recommends that DHS consider the issues raised in the paper to review the existing DHS PIA process. The second states the Committee's assumption that the federated system would permit queries based on only specific PII. In the event that premise is incorrect or changes, the Policy Subcommittee requests the opportunity to revisit the policy paper.

Technology Subcommittee

David Hoffman, Chair of the Technology Subcommittee, summarized his Subcommittee's draft report, highlighting two points: 1) categories of issues that would likely arise with a federated system and questions to ask as well as risks that can arise and 2) the need for significant Privacy Office resources to oversee implementation of the federated system as now envisioned.

Committee Discussion

The Committee discussed both draft reports. Items discussed included:

- perceived inconsistencies between the two papers;
- the possible need for a preamble at the beginning of each paper noting that the papers should be read concurrently;
- the notion that the papers should be considered living documents; and
- whether to edit the technology paper to provide assumptions used when developing it.

The Committee voted to include as an introductory paragraph in the Technology Subcommittee's draft report, paragraph three from Section III of the Policy Subcommittee's draft report. The paragraph now to be included under the title "Privacy Technology Guidance" reads as follows:

Throughout this discussion, we are assuming a system that grants access to specific individuals (or perhaps individuals in specific positions) for specific purposes. More general access would raise a broader set of privacy concerns. We also assume that the system would permit queries based only on specific PII, such as a name, an address, or a phone number. Given this assumption, there is little risk of users searching for potential patterns that conceivably could identify potential persons of interest. A system that would allow such pattern searches raises a far more significant set of privacy issues. Should the proposed system be altered to allow for pattern-based searches, this analysis would need be revisited.

In order to continue its deliberations and in light of time constraints, the Committee voted to reschedule the planned presentation on Media Monitoring by Donald Triner, the Director of Ops Coordination, DHS Office of Operations Coordination and Planning, for a future meeting.

Before calling for a vote on the draft papers, Chairman Purcell opened the floor to public comment on the drafts. Christopher Calabrese, Legislative Counsel for the American Civil Liberties Union (ACLU), commented on the federated information-sharing concept. He noted the ACLU's recent letter to the Secretary of Homeland Security on this issue. He opined that a federated information sharing system could potentially make it possible for 230,000 DHS employees to share information about other DHS employees and therefore DHS must address the risk for widespread surveillance. Mr. Calabrese stated that the ACLU will follow the system development process closely and requested that the ACLU have the opportunity to provide input

throughout that process. He also urged DHS to provide benchmarks or milestones to inform the public about the system's development.

Following Mr. Calabrese's remarks, the Committee proceeded to a vote on the draft papers. The Committee voted to include the two draft papers in one document and to add the following language as a preamble:

This white paper is intended to be responsive to a specific tasking from the Chief Privacy Officer of DHS. This paper is intended to provide guidance based upon the information understood to date by DPIAC and intended to evolve as DHS revises the federated information sharing construct. The document below is to be read concurrently as one paper as well as provide advice and analysis in a timely manner regarding the federated information sharing program that has yet to be built. By requesting DPIAC to issue this guidance early, DHS and the Privacy Office demonstrate their commitment to privacy by design. As the federated information sharing program evolve, so too will this guidance.

There was one dissenting vote and one abstention. A statement expressing the dissenting member's views will be made public along with the final report.

Farewell to Departing DPIAC Members

Following the Committee's vote to adopt the reports as amended, Ms. Callahan recognized five Committee members who are retiring from service on the DPIAC: Chairman Richard Purcell, John Sabo, Lance Hoffman, Ramon Barquin, and Joseph Alhadeff, all of whom were original members of the Committee. Ms. Callahan presented certificates of appreciation to them and thanked them for their contributions and lengthy service to the Department.

Public Comments

Chairman Purcell then provided an opportunity for members of the audience to address the Committee. As there were no further public comments, Chairman Purcell adjourned the meeting at 4:40 pm.

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 DSH that relate to personally identifiable information (PII), as well as data integrity and other privacy-related matters. Materials presented to the Committee, including all Committee reports and recommendations, meeting summaries, and transcripts where available, are posted on the Committee's web page on the DHS Privacy Office website, www.dhs.gov/privacy.