DHS Data Privacy and Integrity Advisory Committee
Public Meeting
July 11, 2011

Committee members in attendance:

Richard V. Purcell, Chairman

Ana I. Anton	Lance Hoffman	Jules Polonetsky
Ramon Barquin	Joanne McNabb	John Sabo
J. Howard Beales III	Lisa S. Nelson	Ho Sik Shin
A. Michael Froomkin	Lydia Parnes	Lisa J. Sotto
Joanna L. Grama	Christopher Pierson	Barry Steinhardt

Also in attendance:
Mary Ellen Callahan, Chief Privacy Officer and Sponsor
Charles Cutshall, Acting Designated Federal Official

Charles Cutshall, in his capacity as the acting Designated Federal Official, called the meeting to order at 10:05 a.m.

Chairman Richard Purcell welcomed Committee members and the public to the fourth Committee meeting of the fiscal year. He announced that the Committee had new members and introduced each of the new Committee members to the public. New members include: A. Michael Froomkin, Joanna Grama, Lisa Nelson, Greg Nojeim, Lydia Parnes, Christopher Pierson, Jules Polonetsky, Ho Shin and Barry Steinhardt.

Ms. Callahan made two administrative announcements:

- DHS published a notice on July 6, 2011 in the *Federal Register* announcing that the DPIAC is now seeking applications to fill positions for terms to expire on January 31, 2014; applications are due by August 15, 2011.
- Due to budgetary constraints, a transcript from the Committee meeting will not be available. Statutorily-required meeting minutes will still be available on the DPIAC page on the DHS Privacy Office's website. This decision will be reevaluated in the new fiscal year.

Ms. Callahan introduced the Deputy Secretary of Homeland Security, Jane Holl Lute.

- Deputy Secretary Lute has over thirty years of military and senior executive experience in the United States government through which she has been actively engaged in efforts to prevent and resolve international crises.
- Before assuming her position at DHS, Deputy Secretary Lute served as Assistant Secretary General of the United Nations, responsible for support to peacekeeping operations. In this capacity, she managed operational support for the second-largest deployed military presence in the world and led rapid-response support to a wide variety of operations and crises in some of the world's most remote, austere, and dangerous environments.

- Prior to joining the United Nations, Deputy Secretary Lute served on the National Security Council staff under Presidents George H.W. Bush and Clinton. She also served as Executive Vice-President and Chief Operating Officer of the United Nations Foundation and the Better World Fund, and headed the Carnegie Commission on Preventing Deadly Conflict. Additionally, Deputy Secretary Lute had a distinguished career in the United States Army, including service in the Persian Gulf during Operation Desert Storm.

Presentation on DHS' International Information Sharing Initiatives
Hon. Jane Holl Lute, Deputy Secretary of Homeland Security

Deputy Secretary Lute updated the Committee regarding the ongoing negotiations with the European Union (EU) to reach a new agreement concerning Passenger Name Records (PNR). To a great extent, the approach being pursued internalizes the Committee's agenda regarding individuals' rights and their entitlement to security of their public information. Deputy Secretary Lute noted that data sharing arrangements must be balanced with security arrangements so that sharing data is never the only end-goal. Rather, it is important to examine the reasons that data is being gathered and shared. While security is a key goal of the U.S. approach to PNR, the goal is not security at the expense of our rights; rather, security is also a right.

Among the fundamental aims for these negotiations are preventing terrorism and building a safe and secure place where the American way of life can thrive, which includes expediting legitimate trade and travel. DHS is approaching the PNR negotiations in a pragmatic way, based on a sound conceptual understanding, experience, and expertise.

Deputy Secretary Lute explained that the United States has years of dealing with PNR without a privacy incident and over time has developed the expertise needed to address the various issues being raised during these negotiations. She used the failed attack in 2009 as an example from which the United States has developed expertise and indicated that there are some lessons that can only be learned from experience. The 2009 attack, for example, demonstrated that the security of the United States is dependent on our ability to help strengthen security systems both at home and abroad. Since air travel to the United States can involve passing through multiple countries, there is an increased risk to the system as a whole if someone is able to infiltrate the system at a weaker point. It is, therefore, important to establish a minimum threshold for security. The new PNR agreement is an effort to both establish such a minimum threshold and strengthen privacy protections, something that the Deputy Secretary views as a win-win for both the United States and the EU.

In 2007, the EU and United States signed a PNR agreement; the United States considered the agreement to be satisfactory, but agreed to renegotiate due to revised European authorities following the Lisbon Treaty approval in the EU. The key question, according to Deputy Secretary Lute, is how to implement a system that incorporates new developments in technology and continues to reinforce the U.S. and EU commitment to privacy and protecting information. She recognized the work of Ms. Callahan and the DHS Privacy Office as being a valuable resource in the ongoing negotiations.

Deputy Secretary Lute provided an overview of some of the specific elements that will be in the final PNR agreement. Specifically, provisions will:

- Establish a clear purpose for the exchange of information.
- Describe ways in which the United States and EU intend to gather, use, and protect information, also setting forth standards, expectations, and tools.
- Describe, for the first time and using ICAO standards, what constitutes PNR.
- Describe the value of PNR as providing predictability for the airline industry.
- Describe what protections will be applied to data (such as masking, physical security controls, and procedures), and reflect a state-of-the-art way of protecting personally identifiable information.

The result of the PNR negotiations will be a robust architecture for protecting individuals' data, with strict controls and oversight, and a commitment by the United States to review and maintain information only for the minimum amount of time necessary.

Deputy Secretary Lute concluded her remarks by stating that she views the PNR agreement positively, as a practical measure that will help keep the travelling public safe while, at the same time, safeguarding people's personal information.

Deputy Secretary Lute then responded to questions and comments from the Committee on a range of topics including the following:

- Her perspective on the specific U.S. and EU privacy concerns that the PNR agreement addressed, and issues that may not be completely resolved;
- The status of the EU-U.S. data protection and privacy umbrella negotiations;
- The DHS and OMB definition of a privacy incident, which is - unauthorized access or disclosure ;
- DHS's plans for keeping pace with advances in technology for anonomyzing and masking data;
- The recognition that constant innovation may be a problem but that the development of a dynamically structured engagement will be able to deal with vulnerabilities as they arise;
- The possibility of a global framework in the future that will allow for protection the collection of U.S. citizen's information by all countries; and
- In negotiations, the necessity to incorporate certain expectations of inclusivity, transparency, and reciprocity of information between countries.

DHS Privacy Officer's Update:

Ms. Callahan provided an update on DHS Privacy Office activities since the DPIAC's May 19, 2011 meeting, including accomplishments of the Privacy Information Sharing and Intelligence, International Privacy Policy, Compliance, Policy, Privacy Technology, FOIA, and Incidents and Inquiries groups.

Privacy, Information Sharing, and Intelligence

DHS concluded five separate Information Sharing Access Agreements with the National Counterterrorism Center (NCTC), covering NCTC's access to DHS's Arrival and departure

System (ADIS), Advanced Passenger Information System (APIS), Electronic System for Travel Authorization (ESTA), Student Exchange and Visitor Information System (SEVIS) and Refugee Applicant Parole System (RAPS) systems.

The Privacy Office is fully integrated into the DHS team that negotiates information sharing agreements. Additionally, these agreements reflected the DPIAC's recommendations in its 2009 White Paper on Information Sharing & Access Agreements, and the principles outlined in the DPIAC's White Paper are now engrained in DHS information sharing policy. For example, each agreement incorporated the DHS Fair Information Practice Principles and contained robust auditing provisions to ensure compliance with privacy obligations.

The Privacy Office's review of NCTC's information-sharing requests included a compliance review of relevant PIAs and SORNs. The existing SORNs contained suitable routine uses. To enhance transparency, the Office issued three PIA updates for SEVIS, APIS, and RAPS. Privacy Office staff also briefed the staff of the House Committee on Homeland Security on DHS information sharing with the intelligence community. These five new agreements were discussed at length.

With the DPIAC's help, DHS has made substantial progress in establishing a repeatable process for receiving and evaluating data requests, and crafting ISAAs that protect the privacy rights of US Persons and other individuals in DHS systems.

With regards to identity management, the Privacy Office continues to make significant contributions towards the Department of Commerce's implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). Two Privacy Office staff members are devoting significant time to the NSTIC implementation to help ensure that privacy protections are embedded into the implementation roadmap.

The Privacy Office is also charged with reviewing intelligence products and reports prepared by the DHS Office of Intelligence and Analysis for any privacy issues. Since the Committee last met, the Office reviewed 38 Homeland Intelligence Reports and 33 finished products, all well within the required time for response to I&A.

International Privacy Policy

The DHS Deputy Secretary led the negotiations for the federal government on the PNR agreement. There is a separate team responsible for negotiating the U.S.-EU "umbrella" Data Privacy and Protection Agreement that would provide a framework for mutual recognition of U.S. and EU privacy systems to facilitate the exchange of law enforcement information. These negotiations are ongoing, and Ms. Callahan, along with the International Privacy Policy team, participated in three negotiating sessions for the umbrella agreement.

IPP is developing two new privacy policy training modules to provide a general understanding of the U.S. privacy framework and to raise awareness of privacy as a foreign policy issue that impacts a number of U.S. Government objectives:

- Training for DHS personnel stationed overseas as part of broader pre-deployment training (with the Federal Law Enforcement Training Center and the DHS Office of International Affairs); and
- Training for other U.S. Government overseas personnel, to include a Data Privacy Policy course at the Foreign Service Institute (with the State Department and the DHS Chief Information Officer).

The Privacy Office continues to work with the Office of International Affairs and DHS components on Canadian initiatives resulting from the February 2011 Beyond the Border Declaration, which calls for increased information sharing while respecting our separate constitutional and legal frameworks that protect privacy.

The Privacy Office is also active in the State Department's International Visitor Program to educate international partners on the U.S. privacy framework, DHS privacy policy, and DHS compliance and FOIA programs.

The next International Conference of Data Protection and Privacy Commissioners will be held in Mexico City on November 2-3. The IPP Director will present on Department safeguards for PII during emergencies and on the privacy protections in the Department's use of social media.

Training

The Privacy Office anticipates introducing the new, interactive online privacy training course for all Departmental staff this fall. The Office is also developing a privacy training and awareness best practices website to benefit all federal agency privacy offices.

Compliance

Between May 19, 2011 and July 5, 2011, the Privacy Office completed 10 PIAs, four SORNs, four Notices of Proposed Rulemakings, four Final Rules, and one Computer Matching Agreement. Additionally, DHS's FISMA score improved from 74% to 77% for PIAs and our SORN score improved from 92% to 95%.

The Privacy Office published a SORN and PIA for the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program and the required security assessments performed by high-risk chemical facilities in fulfillment of Risk-Based Performance Standard # 12 (6 CFR 27.230(a)(12)). This PIA describes the procedures for submitting PII on individuals impacted by this program to NPPD, and also describes NPPD's uses of that PII.

On June 24 and 27, the Privacy Compliance Group held two days of public workshops on privacy compliance requirements. This workshop was designed to accommodate both newer and more experienced privacy professionals. Turnout was high and privacy professionals from DHS as well as several other federal agencies attended.

Policy

The Privacy's Office's Policy group co-chairs the Identity Management Subcommittee of the CIO Council's Privacy Committee and is actively engaged in an array of cross-governmental

identity management issues. The Subcommittee has successfully embedded privacy requirements and guidance in the numerous documents associated with the *Federal Identity, Credential and Access Management Roadmap and Implementation Guidance*.

Privacy Technology

The Privacy Office, with the DHS Chief Information Officer, the Assistant Secretary for Policy, the Director of Records, issued a new Department-wide Privacy Policy Guidance Memorandum entitled *Roles & Responsibilities for Shared IT Services*, which is based on the DPIAC's work on service-oriented architecture. It establishes the foundation for the change to service-oriented technology architecture and a Shared IT Service and enterprise data environment.

This Policy addresses the potential privacy risks from sharing IT services by clarifying the roles and responsibilities of Components sharing IT services, and will help ensure that privacy is embedded in Shared IT Services.

FOIA

The Deputy Chief FOIA Officer completed a comprehensive review of the DHS FOIA program as a whole by meeting with each DHS component-level FOIA Officer to gain a better understanding and share her strategic vision. Three themes emerged from this review that will set the agenda for our FOIA operations in the months to come:

- Reducing backlogged FOIA requests;
- Exploring a DHS enterprise-wide tracking system; and
- Implementing a FOIA Strategic Plan.

The Privacy Office collaborated with the Department of Justice on a training session for the DHS FOIA community on FOIA Exemption 2, which was delivered on June 14, 2011. This targeted training addressed the fundamental change in the way DHS interprets Exemption 2 as a result of the Supreme Court's decision in *Milner v. Dept. of the Navy*, and it helped standardize the application of Exemption 2 across DHS.

DHS has received more FOIA requests in FY 2011 than in FY 2010. To date, DHS has received 107,067 FOIA requests compared to 83,002 requests at this time last year.

Consistent with the Proactive Disclosure Policy Memorandum, the Open Government Directive, and related transparency initiatives, the Privacy Office continues to increase proactive disclosure. DHS has posted FOIA logs for each DHS component, beginning with the January 2009 records and continuing to the present.

Incidents and Inquiries

The Incidents and Inquiries Group is in the process of revising the Privacy Incident Handling Guidance (PIHG). The PIHG is used, along with DHS 4300A – Sensitive Systems Handbook and the Federal Information Processing Standard (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems, to ensure that all DHS privacy and security incidents are identified, reported, and mitigated.

The processes and procedures outlined in the revised PIHG ensure that the Department is responsive to all types of privacy incidents, regardless of the format in which PII is stored. The revised PIHG is expected to be complete by the end of the calendar year.

The third Privacy Incident Handling Quarterly Meeting is planned for late July to provide an overview of privacy incidents at DHS from April through June 2011. This forum provides an opportunity for the component Privacy Officers, Privacy Points of Contact, and the DHS Enterprise Operations Center staff to share information and provide feedback regarding privacy incident management, mitigation, and prevention of privacy incidents.

Following her report, Ms. Callahan responded to questions and comments from the Committee regarding the increased volume of FOIA requests, and provided more detail on the types of requests that the Department receives and what actions DHS is taking to respond efficiently to requests and reduce backlogs.

Presentation on DHS National Protection and Programs Directorate's (NPPD) Privacy Program

Emily Andrew, Directorate Privacy Officer, National Protection and Programs Directorate, U.S. Department of Homeland Security

Ms. Andrew provided an overview of NPPD's mission and the Offices that comprise NPPD. The mission of NPPD is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

The goal of NPPD is to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements. NPPD and its offices focus on the security and resilience of infrastructure that is essential to our economy, national security, public wellbeing, and way of life.

Ms. Andrew was appointed as the NPPD Senior Privacy Officer in September 2010 to lead the effort to fully integrate privacy protections into the NPPD mission and to develop and execute a consolidated strategy for privacy awareness and compliance across NPPD mission areas, consistent with overarching DHS Privacy Office's priorities and policies.

The Privacy Office reports directly to the Under Secretary of NPPD, along with five other offices: the Federal Protective Service, the Office of Cybersecurity and Communications, the Office of Infrastructure Protection, the Office of Risk Management and Analysis, and US-VISIT. These offices cover a wide range of activities that involve or have the potential to involve the collection and maintenance of PII, and privacy protections play an important part in these activities.

US-VISIT is the only office within NPPD that had its own privacy program, which predates the establishment of the NPPD Office of Privacy. Mr. Paul Hasson, US-VISIT's privacy officer, has briefed the Committee on US-VISIT's privacy program on two previous occasions.

Upon joining NPPD, Ms. Andrew worked closely with the leadership and staff of the DHS, NPPD, and US-VISIT offices to leverage DHS and US-VISIT's existing privacy framework and

further integrate privacy into the larger NPPD community. This collaboration ensures effective implementation of privacy policies in furtherance of NPPD's commitment to safeguarding personal information while carrying out mission-related activities.

NPPD's Privacy Office engaged each of the NPPD Offices to ensure that each Office's unique mission is reflected in NPPD's privacy program, and to ensure that the privacy program's mission is fully integrated into efforts to protect and secure personally identifiable information (PII). NPPD also continues to engage with the DHS Privacy Office and its component privacy offices to ensure overall consistency in how privacy is implemented throughout DHS.

Ms. Andrew's first priority was to complete privacy compliance on programs that were moving forward. Due to the unique nature of NPPD's work and its constant collaboration with stakeholders in support of the risk-reduction mission, NPPD has taken a proactive and programmatic approach to privacy compliance. NPPD conducted several programmatic PTAs, PIAs, and SORNS to evaluate the impact various programs as a whole have on privacy and to ensure privacy protections at both the program and system level. NPPD is also in the process of creating a programmatic PIA to tie related programs together, rather than maintaining separate PIAs for each program or system. This approach is expected to increase efficiency.

NPPD is at the forefront of technological development to assist in the protection of the Nation's critical infrastructure and key resources. The Privacy Office works to incorporate fair information practices into new technological developments and programs that utilize technology in ways that affect PII. NPPD's Privacy Office has worked on several key initiatives involving the use of technology, particularly with regards to NPPD's cybersecurity programs, to ensure that privacy is embedded into the technologies being utilized for cyber detection and to mitigate the risks associated with securing our Nation's infrastructure from cyber attacks.

In conjunction with National Cybersecurity Awareness Month in October, NPPD launched the Stop. Think. Connect. campaign, which is a national public awareness effort to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about developing safe online habits. The campaign utilized social media to disseminate information and engage the public to participate in its programs. NPPD's Privacy Office worked closely with the campaign to ensure that social media practices included privacy protections.

The NPPD Privacy Office has worked to increase awareness of privacy within NPPD by providing privacy training to all NPPD employees and contractors as well as targeted privacy training to specific groups, and launching an internal privacy website. Additionally, US-VISIT held its third Annual Privacy Awareness Week in October. Next year, this event is expected to be extended to all of NPPD.

NPPD's focus this coming year will be to continue to systematically maintain the PII inventory, document compliance, and conduct privacy training and awareness throughout NPPD.

Following her report, Ms. Andrew responded to questions and comments from the Committee regarding the status of NPPD's programmatic PIA.

Public Comments

Chairman Purcell opened the floor for public comments at 12:10 p.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 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, 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.