DHS Data Privacy and Integrity Advisory Committee
Summary of Public Meeting
March 18, 2010, Washington, DC

Committee members in attendance:

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

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 8:30 a.m.

DHS Privacy Officer's Update:
Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security

Ms. Callahan highlighted the following accomplishments of the DHS Privacy Office during her tenure as Chief Privacy Officer:

- Approved 518 Privacy Threshold Analyses (PTAs), 68 Privacy Impact Assessments (PIAs), and 62 System of Records Notices (SORNs).
- Approved 10 fusion center privacy policies; 6 additional fusion center privacy policies are pending review.
- Conducted 12 outreach events.
- Gave 25 presentations to government and public audiences.
- Met with every DHS component at least twice. Discussions included the requirement that components have privacy officers.

Ms. Callahan also provided an update on the activities of the DHS Privacy Office since the Committee last met in December, including accomplishments and updates on the work of the DHS Privacy Office's policy, international privacy policy, privacy technology and intelligence, compliance, and FOIA groups.

Policy Group:

- Helen Foster joined the DHS Privacy Office as a Senior Privacy Analyst and will focus on building privacy protections in information sharing agreements both within DHS and with external partners.
- Revised draft DHS information sharing guidance, including DHS Information Sharing Access Agreement (ISAA) Templates and Guidebook and the Data Access Request

process. Revisions address concerns and recommendations raised in the Committee's 2009 White Paper on DHS Information Sharing and Access Agreements. Draft documents are currently being vetted within DHS. Ms. Foster will update the Committee in May.

- Supporting White House initiative to develop a National Strategy for Secure Online Transactions, which focuses on strategies to implement identity management solutions to enhance the privacy and security of online transactions across the government and private sector.

International Privacy Policy Group:

- As follow up to Secretary Napolitano's recent meeting in Spain with the German Justice Minister, Ms. Callahan traveled to Brussels, Strasbourg, Amsterdam, The Hague, and Berlin to address European partner criticisms and correct misconceptions regarding DHS privacy policies, and to build support for DHS information sharing with international partners.
- Hosted an Australian delegation with the Department of State and Department of Justice (DOJ), to discuss the Preventing and Combating Serious Crime and Homeland Security Presidential Directive-6 Agreements. Ms. Callahan and the DOJ Chief Privacy and Civil Liberties Officer spoke on the United States privacy framework and their respective agencies' privacy policies and practices.
- Hosted a delegation led by the European Union (EU) Commission for their review of DHS privacy practices under the 2007 Passenger Name Record (PNR) Agreement. The review included site visits to the National Targeting Center and the Passenger Analytic Unit at Dulles Airport, as well as comprehensive briefings by DHS Customs and Border Protection (CBP) and the DHS Privacy Office Compliance Group. The EU delegation's report is expected in the spring.
    - In preparation for review, the DHS Privacy Office updated the December 2008 Report Concerning Passenger Name Records derived from flights between the U.S. and the EU 2008. The updated report finds that CBP has taken action to address all six of the outstanding recommendations contained in the 2008 Report and that CBP continues to comply with the terms of the 2007 U.S. - EU PNR Agreement.
- Participated as an observer at a meeting of the Council of Europe's Consultative Committee on Convention 108, in sessions on transatlantic information sharing, protection of personal information with regard to data mining, and potential revisions to the Convention. This was the first time the United States has participated; the United States was granted observer status in February 2010.

Legislative and Regulatory Analysis Group:

- Continued involvement in the Department’s work with state and local fusion centers to ensure privacy protections are in place.
- Conducted ongoing reviews of individual fusion center privacy policies to confirm that they are "at least as comprehensive" as the privacy guidelines issued by the Program Manager - Information Sharing Environment. To date, the DHS Privacy Office has approved 10 policies. 2010 DHS Grant Guidance requires fusion centers to complete privacy policies as a condition of future grant awards.

- Attended the National Fusion Center Conference in New Orleans. Ms. Callahan participated as a panelist for Privacy 101 and addressed a private meeting of fusion center directors.
- In conjunction with the DHS Office for Civil Rights and Civil Liberties, the DHS Privacy Office is providing ongoing support for fusion center privacy and civil liberties training.

Privacy Technology and Intelligence Group:

- The White House recently issued an unclassified description of the Comprehensive National Cybersecurity Initiative (CNCI). A classified PIA was completed for the CNCI Initiative 3 Exercise.[1]
- Published a PIA on a proof of concept pilot project of the EINSTEIN 1 capabilities with United States Computer Emergency Readiness Team (US-CERT) and the State of Michigan.
- Worked with the DHS National Protection and Programs Directorate to publish a white paper on DHS Computer Network Security and Privacy Protection.
- The white paper and both PIAs are posted on the DHS Privacy Office website.

Compliance Group:

- Assigned a near full-time administrative assistant to assist in managing compliance documentation through the new Compliance Tracking System.
- The DHS Privacy Office plans to release a new PIA template and guidance during its annual Privacy Compliance Workshop on June 10.
- Collaborated with the DHS Privacy Office Director of Privacy Incidents and Inquiries and Associate Director of Communications and Training to improve the Office's quarterly reporting required by Section 803 of the 9/11 Commission Act, by adding narrative examples of the types of reviews conducted and complaints received, and by clarifying categories of complaints and their dispositions.
- Drafted two social media PIAs covering networking interactions and informational push (non-interactive) social media, respectively. The DHS Privacy Office is also working with the DHS Office of General Counsel, Chief Information Security Officer, and Office of Public Affairs to develop a social media compliance process review.
- Finalizing a process for Computer Matching Agreements (CMA) and establishing a formal Data Integrity Board as required by the Privacy Act.
- Supporting the federal Chief Information Officer (CIO) Council's Identity, Credential, and Access Management Subcommittee's work on identity management by drafting a model PIA for federal agencies considering the use of commercial credentials to register individuals at federal websites.

Privacy Incidents and Inquiries Group:

- Briefed House Homeland Security Committee professional staff on 2009 accomplishments regarding privacy incident management, on the DHS electronic Compliance Tracking System, and the DHS Privacy Office's role in the DHS Traveler Redress Inquiry Program (DHS TRIP).

[1] The unclassified version of the PIA was published on March 18, 2010, shortly after the meeting adjourned.

- In response to suggestions from Committee members, queried component Privacy Officers and Privacy Points of Contact about their privacy complaint handling procedures. This information will assist in identifying best practices for the DHS components and assess feasibility of reporting additional data in the Section 803 Report.
- Hosted the second DHS Privacy Incident Handling Quarterly Meeting to gain better understanding of the causes of privacy incidents and complaints.

Freedom of Information Act Group:

- Hired 6 new FOIA specialists and a new administrative specialist will be on board shortly.
- Published the DHS FY2009 FOIA Report to the Attorney General and the Department's first Chief FOIA Officer's Report.
- Made substantial continued progress in reducing the Department's backlog of FOIA requests.
- The DHS Privacy Office is taking an aggressive approach to proactively disclosing information in keeping with the President's Open Government Memorandum.
- Supported significant enhancements to DHS online FOIA Reading Rooms. DHS has disclosed over 500 documents and new information is posted on many DHS sites on a weekly basis.

Presentation on Computer Network Security and Privacy Protections in DHS

Admiral Michael Brown, Deputy Assistant Secretary for Cybersecurity and Communications, DHS National Protection and Programs Directorate

Admiral Brown provided background on National Security Presidential Directive 54, Homeland Security Presidential Directive 23 and the Comprehensive National Cybersecurity Initiative (CNCI), focusing on a comprehensive overview of CNCI's 12 initiatives. He discussed DHS' leadership role within CNCI in the areas of cybersecurity and protection of Americans' privacy and other rights, including PIAs on Einstein 1, Einstein 2, and the proof of concept pilot project of the EINSTEIN 1 capabilities with US-CERT and the State of Michigan; Civil Liberties-Privacy Community Meetings; and the DHS Privacy Office's and Office for Civil Rights and Civil Liberties' role in providing annual training to US-CERT personnel. He discussed the mission of the National Cybersecurity and Communications Integration Center, which will unify efforts of the National Coordinating Center, US-CERT, the DHS Office for Intelligence and Analysis, and the National Cybersecurity Center. He also discussed the role of the National Cyber Incident Response Plan (NCIRP), which will be tested during the Cyber Storm III exercise to be held in September 2010. Admiral Brown invited discussion from the Committee and responded to members' questions after concluding his presentation.

Presentation on DHS Participation in Federal Interagency Privacy Initiatives

Toby Levin, Senior Advisor and Director of Policy and Education, DHS Privacy Office

Ms. Levin discussed the work of the federal CIO Council's Privacy Committee, which is co-chaired by the DHS Chief Privacy Officer, the Department of Veterans Affairs Assistant Secretary of Information and Technology, and the DOJ Chief Privacy and Civil Liberties Officer. Lynn Parker from the DHS Privacy Office serves as the Committee's executive assistant. The Privacy Committee is the principal interagency forum for improving agency practices for the protection of privacy, and serves as the interagency coordination group for Senior Agency Officials for Privacy and Chief Privacy Officers in the federal government. Ms. Levin discussed the Committee's five subcommittees: Best Practices; Development and Education; International Privacy; Web 2.0; and Identity Management. John Kropf, DHS Deputy Chief Privacy Officer, co-chairs the International Privacy Subcommittee. Ms. Levin serves as co-chair for the Best Practices Subcommittee, which is currently addressing how to embed privacy principles in the federal enterprise architecture. Ms. Levin responded to questions and comments from the Committee after concluding her presentation.

Subcommittee Updates

Data Integrity and Information Protection Subcommittee Co-Chair Ramon Barquin presented a draft white paper on recommendations for the PIA process for Enterprise Services Bus (ESB) Development, for deliberation and vote by the full Committee. Several amendments were introduced and discussion followed. The Committee voted unanimously to approve the draft as amended. The white paper includes the following recommendations to the DHS Secretary and Chief Privacy Officer:

1. Develop rigorous policies, procedures, technical mechanisms and controls to qualify individuals and services requesting access to the ESB including:
   - qualifying and authenticating all individuals accessing the ESB;
   - qualifying and authenticating services that request data from and provide data to the ESB; and
   - acceptable uses of the data distributed by the ESB, including conditions necessary to protect sensitive personal information.

2. Develop a mini-PIA process that is applicable whenever new purposes are planned for an existing ESB.

3. Develop policies, procedures, technical mechanisms and controls under which services and sub-services may combine data for specified purposes; include procedures to qualify the authority for access to the data as well as to assure the protection of the resulting data from unauthorized use or disclosure.

4. Support the development, maintenance and updating of policies, procedures, technical mechanisms and controls to encrypt sensitive data in both resting and transmission states.

5. Review ESB audit capabilities, including access, data requests, data supplies, services uses and security safeguards to assure compliance with the DHS Fair Information Practice Principles (FIPPs).

6. Consider including the following requirements in the PIA for an ESB:

- Describe the ways the ESB complies with the FIPPs;
- Describe how the ESB improves compliance with the FIPPs over current systems it replaces;
- Describe the controls in place to qualify an individual's access to the ESB;
- Describe the information security safeguards the ESB implements to protect data from unauthorized use, disclosure, corruption or loss;
- Describe how the ESB supports data retention standards of the Department; and
- Describe the audit protocols supported by the ESB and how are they enforced, reported and monitored.

The white paper also includes a list of questions for consideration in conducting a privacy impact assessment when planning services hosted on an existing ESB.

Privacy Architecture Subcommittee Co-Chair Joanne McNabb and Data Acquisition and Use Subcommittee Chair David Hoffman presented a draft white paper on the elements of effective redress programs, for deliberation and vote by the full committee. Several amendments were introduced and discussion followed. The Committee voted unanimously to approve the draft as amended. The white paper includes the following recommendations for developing, deploying, and monitoring an effective redress program:

- Assign accountability for the privacy redress process to a single owner with responsibility for developing and managing policies and processes that make the program accessible, understandable and fair;

- Provide information to the public that explains redress seekers' rights, the process for complaining or seeking redress, a general timeline for the process, and the privacy policy regarding the personal information used in the process;

- Provide descriptive information on the process in plain language, in an easy-to-read format, in languages appropriate for the people seeking redress, at points of contact with individuals, on organization websites, and in other available venues;

- Develop and deploy a training program that educates employees, contractors, vendors and others as appropriate about the redress policies, procedures, standards, and access points;

- Ensure that corrections or annotations are propagated throughout all primary and secondary systems, to prevent the same information from producing an adverse impact in the future;

- Set service standards for logging redress complaints and providing timely responses, and promote transparency and accountability by including the standards in publicly available documents;

- Develop administrative and technical support for the redress process to integrate it into the regular workings of the organization; and

- Establish, administer and monitor an appeals process designed for transparency and fairness; develop and implement an effective redress appeals process that provides individuals with confidence that the ultimate reviewer is appropriately impartial.

Public Comments and Questions to the Committee

Chairman Purcell opened the floor for public comments at 12:30 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.