The Privacy Office
Homeland Security

Privacy Matters

Chief Privacy Officer's Message

It is an honor to serve as the Chief Privacy Officer for the Department of Homeland Security. I thank my predecessors and my colleagues here at the Privacy Office for working so diligently to achieve our mission to imbue DHS with a culture of privacy.

We believe that respect for individual privacy is a core value of our free society and one that the department is fighting to protect. Today, more than ever, we know that privacy and security are inseparable and must be integrated if the department's programs, and its mission, are to succeed.

To achieve our mission, we work closely with our colleagues in the department to ensure that privacy is considered throughout the lifecycle of each information system or program. From the technology investment review process to the privacy impact assessments required for the OMB budget investment process, Privacy Office guidance is critical to ensuring that the technologies and programs used by DHS sustain privacy protections.

By addressing privacy upfront, at the earliest stages of system and program development, the Privacy Office seeks to enhance the public trust that we believe is critical to the department's success.

Thank you for supporting the Privacy Office and its mission. I look forward to working with you as we continue to infuse DHS with a culture of privacy.

-Hugo Teufel III
Chief Privacy Officer

Inside This Issue, Summer 2006

Privacy Office Continues Popular Workshop Series

Overflow Crowd Attends PIA Workshop, Learns about Compliance Processes

WASHINGTON— On June 15, 2006, the Department of Homeland Security (DHS) Privacy Office continued its popular public workshop series hosting, "*Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments.*" The workshop explored the policy, legal, and operational frameworks for Privacy Impact Assessments (PIAs) and Privacy Threshold Analyses (PTAs).

An audience of over 250 people, mostly representing DHS and other federal agencies and departments, participated in the workshop. Transportation Security Administration (TSA) Assistant Secretary Kip Hawley opened the workshop as the keynote speaker and discussed TSA's success incorporating privacy into its operations. Hawley's remarks underscored the importance of building privacy into the enterprise setting and confirmed the importance of the workshop to the department and the audience.

The workshop's program consisted of two sessions. The morning session included two discussion panels. The first panel, consisting of federal government and private

See WORKSHOP, page 2

Need Help Doing PIAs for your C & A Processes?

Contact us at:

www.dhs.gov/privacy,

Or on email at:

pia@dhs.gov

DHS Security Conference Highlights Office Outreach

Chief Privacy Officer and Senior Staff Speak in Baltimore, MD

BALTIMORE—The Department of Homeland Security (DHS) Privacy Office shared its perspectives on privacy with a large audience of colleagues at the 2006 DHS Security Conference and Workshop: *Raising the Bar for Security*, in Baltimore, Maryland, in August.

DHS Chief Privacy Officer Hugo Teufel III opened the conference with his keynote speech explaining the Privacy Office, its mission, its role, and the importance of protecting privacy.

"We frame the mission as securing the homeland while protecting privacy," Teufel said.

Teufel noted the connection between privacy and security, stressing that the two are inseparable and must be integrated into DHS programs if they are to succeed.

Toby Levin, the Privacy Office's senior advisor, discussed federal guidance for data breach response planning. She outlined some of the recent measures taken to address data breaches including the President's Identity Theft Task Force, several OMB and GSA actions and initiatives, and recently introduced federal legislation.

Rebecca Richards, the Privacy Office's director of privacy compliance and Nathan Coleman, privacy compliance coordinator for the office, each gave a presentation on the requirements for Privacy Impact Assessments (PIA). Each discussed the PIA process, the content included in a PIA, and writing a PIA for a public audience. ⌘

Workshop— Continued

sector privacy professionals, discussed how their organizations operationalize privacy in the course of their everyday duties. Panelists sought to illustrate how organizations move from privacy as a value, policy, or statutory mandate to making privacy an integral part of its day-to-day operations. Each panelist offered examples of programs and technologies they employ to illustrate how to move beyond privacy as a concept to privacy as an organizational practice.

The second panel focused on compliance with federal privacy requirements, including system of records notices, PIAs, certification & accreditation under the Federal Information Security Management Act, and the Office of Management and Budget annual budget process. Panelists from DHS and other federal agencies and departments offered practical examples illustrating how these legally required privacy tools are used. Panelists explained that these tools assist in minimizing the amount of data that a program collects by ensuring that its managers understand their mission and how data minimization applies to it. Use of these tools helps assure that program designers and technical staff are only collecting or sharing the limited amount of information necessary to accomplish a program's goals.

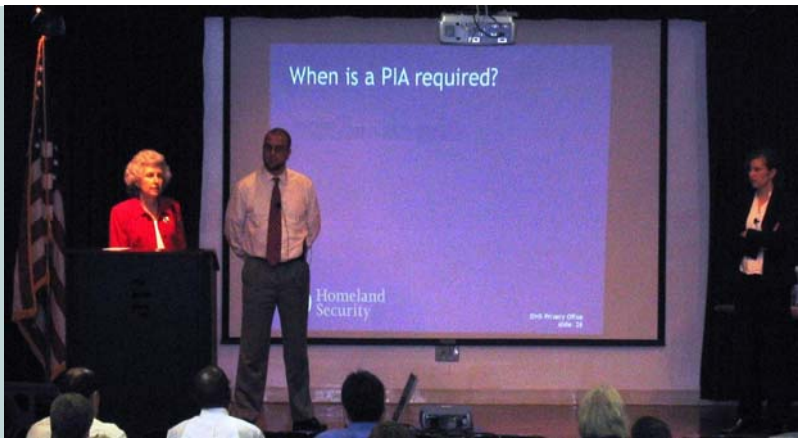
In the afternoon, the Privacy Office's Director of Privacy Compliance Rebecca Richards and Privacy Compliance Coordinator Nathan Coleman presented a tutorial on writing PIAs and PTAs. The tutorial illustrated a step-by-step approach to drafting and submitting a PIA using the Privacy Office's PIA guidance.

The Privacy Office hosted a second PIA tutorial on July 12, 2006, to accommodate the overwhelming popular demand. An audience of over seventy people attended. Senior Advisor Toby Levin joined Richards and Coleman in the presentation.

A full transcript of the workshop is available at: www.dhs.gov/privacy.⌘

Privacy Office Outreach

September 20, 2006
Data Privacy and Integrity Advisory Committee Meeting; Washington, DC
September 25, 2006
Rebecca Richards: American Society of Access Professionals; Washington, DC
September 26, 2006
Ken Mortensen: Global Identity Infrastructure Summit; London, United Kingdom
September 28, 2006
Peter Sand: Defense Science Board Task Force on Defense Biometrics; Arlington, VA
Ken Mortensen:IT and The Law, Dealing With Privacy and Compliance; Columbus, OH
October 18, 2006
Hugo Teufel III: IAPP Speakers Dinner; Toronto, Canada
December 6, 2006
Data Privacy and Integrity Advisory Committee Meeting; Miami, FL



Privacy Office staff addresses the audience at the July 2006 PIA tutorial in Washington, DC.

Privacy & Technology Investment

Promoting Privacy Protections in the Investment Review Process

The U.S. Department of Homeland Security (DHS) investment review process adheres to the Capital Planning and Investment Control (CPIC) requirement to use a systematic approach to select, manage, and evaluate information technology investments. The Enterprise Architecture Board (EAB), supported by the Enterprise Architecture Center of Excellence (EACOE), is one of the primary vehicles for fulfilling this CPIC requirement. The DHS Privacy Office works within this process to ensure the technologies the department uses sustain privacy protections as mandated by Section 222 of the Homeland Security Act.

The EACOE, which is led by the DHS Enterprise Architecture Office on behalf of the DHS Office of the Chief Information Officer (OCIO), reviews all proposed technology initiatives to ensure that new technology initiatives align with departmental technology strategies and platforms. The EACOE fulfills the department's responsibility under the CPIC requirements through technology reviews and administrative enforcement. As part of the EACOE process, the Privacy Office reviews technology investment proposals for privacy implications and votes to continue or stop the progress of such proposals. The Privacy Office review is meant to ensure that the privacy compliance assessment and documentation process starts as early as possible.

The Privacy Office is developing privacy technology guidance for integration into the preparation process leading up to the EACOE review process. The guidance will create privacy protection and awareness requirements for each of the milestone decision points of the overall DHS investment review process. When implemented, the Privacy Office's privacy technology guidance will include a privacy standard of practice, a measure of success, and specific privacy checklists for each decision point that will guide and inform the development of proposed technology investments. Successful adoption of this guidance should result in fewer privacy issues arising in proposed technology investments reviewed by the Privacy Office and the EACOE and an overall improvement in the initial drafts of all privacy compliance documentation across the department.

As the Privacy Office completes its draft privacy technology guidance, it continues to partner with the EACOE, EAB, OCIO and the other organized efforts across the department to manage the technology investment review process and ensure that each technology initiative is fully privacy compliant. Through these ongoing efforts, those involved learn and "own" a little more privacy awareness, so that with each subsequent project, the technology proponents, and even the technologies themselves may become more protective of privacy.⌘

Data Privacy and Integrity Advisory Committee Visits Bay Area

State Perspective, Border Management and Enforcement Talks Highlight Committee Meeting

SAN FRANCISCO— On June 7, 2006, the DHS Data Privacy and Integrity Advisory Committee visited the Bay Area, hosting its second quarterly meeting of 2006 at the Clift Hotel.

Robert Samaan, deputy director of the California Office of Homeland Security (COHS) addressed the committee regarding its mission and functions. He said the mission of California's homeland security office "matches the national strategy of homeland security." Samaan identified the six functions of the office as information analysis and warning, protecting critical infrastructure and key resources, training and exercise, strategic planning, grant funding administration, and citizen preparedness. He also noted that California has taken steps to "ensure that privacy is taken seriously," including developing the State Terrorism Threat Advisory Group (STTAG). The STTAG provides the COHS and the California Department of Justice with advice on the development and practices of California's State Terrorism Threat Assessment Center and regional centers.

"Privacy is of the utmost importance to our office and other officials around California and the United States," Samaan said.

Border Management and Enforcement Discussed

U.S. Immigration Customs Enforcement (ICE) Special Agent Charles DeMore and US-VISIT Privacy Officer Steve Yonkers addressed the committee on border management and enforcement and the use of radio frequency identification (RFID) in the immigration and border management enterprise.

DeMore spoke on border management by first identifying the different types of borders: land, air, sea and cyber. He discussed the importance of thinking about borders as a "virtual reality" as well as a physical one, noting the potential effectiveness of sending technology and information to our nation's enemies. DeMore provided an overview of the three operational areas of ICE: finance, public safety and national security. In addition, he briefly discussed the Secretary's "blueprint" for immigration reform, the Secure Border Initiative.

DeMore said that population growth through immigration is likely to happen, but must be done in "a constructive and thoughtful manner."

Yonkers began his remarks by defining the goals of US-VISIT: enhancing the security of citizens and visitors, facilitating legitimate travel and trade, ensuring the integrity of the immigration system, and protecting the privacy of visitors. He also discussed implementing US-VISIT 2C, which is the proof of concept whereby RFID tags are embedded into I-94 forms, highlighting the opportunity to study how RFID will help address the challenges at land borders by providing information to border officers prior to interaction with travelers. Yonkers also noted that although RFID is extremely helpful, it is important to maintain the privacy of the traveler. To that end, he said, passive RFID will "allow us to preposition the information" without having personally identifiable information in the actual RFID tag.

"We need to be able to make people trust us and that means we have to be transparent" and let them know what we are doing and get their feedback, Yonkers said.

Experiences With Closed Circuit Television

Clive Norris, deputy director at the Centre for Criminological Research at Sheffield University in England, spoke to the committee about closed circuit television (CCTV) and its impact in Britain. He noted that the use of CCTV began in retail stores to prevent shoplifting, and with traffic cameras monitoring red lights.

Norris presented four benefits of CCTV in Britain: crime reduction, tapes for use as post-investigative resources, allowing authorities to examine situations to determine how to react, and criminal confessions. Norris said that although CCTV provides valuable information, research shows there are also "drawbacks", such as camera operators targeting people instead of behaviors.

Panels Discuss Privacy in Public and ID Authentication

The committee hosted two panels, one on the *Expectations of Privacy in Public Spaces* and the other on *Identity Authentication*.

The *Expectations of Privacy in Public Spaces* panel included Nicole Wong from Google, Inc., Deirdre Mulligan from the University of California at Berkeley, and Lillie Coney from the Electronic Privacy Information Center. Panelists discussed the importance of privacy in public places and on the internet, as well as the impact of video surveillance.

The *Identity Authentication* panel included George Valverde from the California Department of Motor Vehicles, Jim Dempsey from the Center for Democracy and Technology, and Jonathan Fox of Sun Microsystems. Panelists discussed REAL ID, valid authenticators, and digital identity management.

For meeting transcripts or more information on the Data Privacy and Integrity Advisory Committee, visit www.dhs.gov/privacy.⌘

Advisory Committee Welcomes New Members: Diversity of Experience, Expertise Highlighted

WASHINGTON, DC—The DHS Data Privacy and Integrity Advisory Committee will welcome six new members in September:

Thomas Boyd, partner, Alston & Bird LLP in Washington, DC; Renard Francois, attorney, Bass, Berry & Sims in Nashville, Tennessee; Neville Pattinson, director of marketing and government affairs, Gemalto in Austin, Texas; Lawrence Ponemon, chairman and founder, the Ponemon Institute in Tucson, Arizona; Ana Anton, associate professor of software engineering, North Carolina State University in Raleigh, North Carolina; and Mary DeRosa, senior fellow, the Center for Strategic and International Studies in Washington, DC.

Since its inception, the committee has sought to represent the great diversity of interests and expertise found within the privacy community, and these new appointees continue that practice. The new cohort of committee members includes officials from the administrations of presidents Reagan, George H.W. Bush, and Clinton; privacy lawyers; technology experts; and representatives from the non-profit sector and academia.

For the above mentioned cohort, each new member's term expires in 2010.⌘

Privacy Office Staff

Hugo Teufel III
Chief Privacy Officer and
Chief FOIA Officer

Kenneth P. Mortensen
Acting Chief of Staff

Toby Milgrom Levin
Senior Advisor

John Kropf
Director, International Privacy Policy

Peter E. Sand
Director, Privacy Technology

Rebecca Richards
Director, Privacy Compliance

Catherine Papoi
Acting Director, Departmental Disclosure and FOIA

Sandra L. Hawkins
Administrative Officer

Lane Raffray
Special Assistant to the Chief Privacy Officer

Shannon Ballard
International Privacy Analyst

Lauren Saadat
International Privacy Analyst

Nathan Coleman
Privacy Assessment Coordinator

Erica Perel
Attorney-Advisor
Office of the General Counsel

DHS Privacy Office Contract Support

Cathy Lockwood
Senior Policy Analyst

Kathleen Kavanaugh
Analyst

Tamara Baker
Event Executive

Rachel Drucker
PIA Specialist

Catrina Robinson
Privacy Threshold Analysis Processor

Sandra Debnam
Administrative Assistant

Erin Odom
Administrative Assistant

Vania Lockett
Senior FOIA Specialist

Loren Clark-Moe
FOIA Specialist

Mark Dorgan
FOIA Specialist

Stephanie Kuehn
FOIA Specialist

James Larsen
FOIA Administrative Specialist

Component Privacy Officers

Steve Yonkers
Privacy Officer, US-VISIT

Peter Pietra
Privacy Officer, TSA

Website: http://www.dhs.gov/privacy/
Email: privacy@dhs.gov
Telephone: (571) 227-3813
Facsimile: (571) 227-4171
FOIA Facsimile: (571) 227-1125

Meet the New Privacy Office Staff

Shannon Ballard

Shannon Ballard joined the DHS Privacy Office as an International Privacy Analyst. As a partner in a job-share arrangement with Lauren Saadat (see below), Ballard is responsible for international policy development and advising senior staff on international privacy law and policies. Her portfolio includes privacy issues relating to the Asia Pacific Economic Cooperation (APEC) member economies; the Berlin Group, an international working group on data protection and communications; and biometrics.

Prior to joining the Privacy Office, Ballard served in a job-share with Saadat at the U.S. Department of Commerce. As co-administrator of the U.S. - European Union (EU) Safe Harbor framework, Ballard managed certifications and facilitated commerce for over 970 U.S. companies. She also covered data privacy issues in the EU, South Korea, and Africa. While at the Department of Commerce, Ballard led privacy and other e-commerce related matters for the bilateral U.S.-Japan Regulatory Reform Initiative, before taking over the Safe Harbor portfolio.

Ballard has almost 15 years of experience with international trade and policy issues.⌘

Lauren Saadat

Lauren Saadat joined the DHS Privacy Office as an International Privacy Analyst as a job-share partner with Shannon Ballard. Like Ballard, Saadat is responsible for international policy development and advising senior staff on international privacy law and policies, including DHS compliance with international agreements.

Previously, Saadat was co-administrator of the Safe Harbor framework on commercial, personal data flows between the U.S. and EU for the U.S. Department of Commerce. In addition, she conducted research and analysis on the international economic, trade and policy implications of electronic commerce. While at Commerce, Saadat received the Department's second-highest honor, the Silver Medal Award, for her work on China.

In 2001, Saadat authored "The Lawyer's Guide to China's Technical Regulations for Imported Products," an American Bar Association publication. She has both an M.A. in East Asian Studies and a J.D. from Washington University in St. Louis, Missouri.

Saadat is a lawyer admitted to the State of Missouri Bar. She speaks Mandarin Chinese and Spanish.⌘

Nathan Coleman

Nathan Coleman joined the DHS Privacy Office as a Privacy Compliance Coordinator. Coleman comes to the Privacy Office from SRA International where he served as a Privacy Analyst detailed to the Privacy Office. Since February 2005, he has worked with the Director of Privacy Compliance to manage the Privacy Impact Assessment process, develop the Privacy Threshold Analysis and deploy it into the Certification and Accreditation process, draft and update the DHS PIA Guidance, and enforce DHS policy.

Prior to joining the Privacy Office as a contract employee, Coleman worked in criminal law and procedure at the Hamilton County, Ohio, Public Defender's Office.

Coleman holds a B.A. in English Literature from the University of Missouri-Kansas City, and a J.D. from the University of Cincinnati College of Law. He is a member of the Virginia and Ohio State Bars.⌘

Talk to us!

Need help writing PIAs? Have a question about privacy? Or would you like to have the DHS Privacy Office make a presentation to your organization, please contact us at (571) 227-3813. Feel free to contact us via email at privacy@dhs.gov.

If you would like to make a presentation to the Privacy Officers and Freedom of Information Act Officers for the Department of Homeland Security, please contact the DHS Privacy Office at (571) 227-3813 or privacy@dhs.gov. Please note that topics should be related to privacy or FOIA issues, rather than privacy or FOIA products or services.