The Privacy Office
Homeland Security

Privacy Matters

Chief Privacy Officer's Message

Since the inception of the DHS Privacy Office, it has been our mission to support the Department in its efforts to protect the homeland, while at the same time safeguarding the privacy of individuals, and particularly, the individual's personal information. This is our mission, and each day we here at the DHS Privacy Office work diligently to achieve it.

Over the course of the spring, we have welcomed a new Secretary and Deputy Secretary to the Department, both of whom support our office and its mission, and we thank them for it. We have strengthened our already proficient staff by adding new, incredibly qualified staff. We have witnessed the inauguration of the Data Privacy and Integrity Advisory Committee, and are looking forward to its recommendations for improving policy and implementing "best practices" as we constantly strive to achieve our mission better. In addition, we have continued to reach out to our partners around the globe, because effectively protecting the homeland requires the strong bonds of international collaboration.

As always, we will continue to foster collaboration from our colleagues within the Department, privacy advocates, citizens, and the international community, as we remain ever vigilant in our pursuit of strong privacy protections while protecting our homeland.

We thank you for your support of our office during its first two years, and we look forward to continued collaboration with you.

-Nuala O'Connor Kelly, Chief Privacy Officer

Inside This Issue, Spring 2005

The Beginning: The Privacy Advisory Committee

First Public Meeting of the DHS Data Privacy and Integrity Advisory Committee a Huge Success

WASHINGTON, DC—On April 6, 2005, the Data Privacy and Integrity Advisory Committee for the U.S. Department of Homeland Security held its inaugural public meeting at the Mayflower Hotel in downtown Washington, DC. The committee's objective is to advise the Secretary and the DHS Privacy Officer on issues within the department that affect individual privacy, and to guide the department in implementing a comprehensive privacy framework to strengthen individual privacy protections while securing the nation.

Nuala O'Connor Kelly, Chief Privacy Officer for the department, and the sponsor of the advisory committee, opened the meeting with a resounding call to action. She remarked that the committee was created to formalize the department's relationships with the public to bring forward the public's thoughts and concerns about the department, and to also advise the department on the best learning and best practices from the private sector.

The inaugural meeting of the committee was honored with bipartisan support from Capitol Hill, with remarks by both the Honorable Bennie Thompson (MS-D), Ranking Member of the House Committee on Homeland Security, and the Honorable Chris Cannon (UT-R), Chairman of the Subcommittee on Commercial and Administrative Law of the House Judiciary Committee.

See FIRST MEETING, page 2

Data Privacy and Integrity Advisory Committee:
On the web at,
www.dhs.gov/privacy
On email at,
privacycommittee@dhs.gov

Privacy Office Outreach to Europe

Privacy Office Continues Privacy Dialogue With Europeans

The DHS Privacy Office continued its dialogue with Europe this spring, visiting the European Union (EU) in May to represent the Department at events in Ireland, Belgium, and France.

On May 20, 2005, Chief Privacy Officer Nuala O'Connor Kelly and Chief of Staff and Senior Advisor for International Privacy Policy Maureen Cooney visited the Institute of European Affairs in Dublin, Ireland. Kelly gave the keynote address before a diverse audience representing members of parliament, government departments, the judiciary, law enforcement, business interests, and others.

In her address, Kelly provided an overview of her role as Chief Privacy Officer for DHS and the privacy framework that provides the underpinnings of privacy policy in the United States, including the Privacy Act of 1974, the Freedom of Information Act, and the E-Government Act of 2002. In addition, she noted examples of cross-border information sharing programs currently underway, such as the U.S.-EU PNR Agreement and Enhanced International Travel Security (EITS),

See OUTREACH, page 2

First Meeting

Continued from front page

The meeting featured a presentation from DHS Deputy Secretary Michael P. Jackson, who reiterated the department's support for both the creation of the committee and the autonomy of the DHS Privacy Office to ensure that operations of the department include privacy protections for the public. Following Deputy Secretary Jackson, a number of component representatives made presentations to the committee, and each echoed the sentiments of the Deputy Secretary and invited the committee to assist them in securing the nation without eroding fundamental privacy protections.

The afternoon session included panels of renowned privacy experts including James Dempsey, Parry Aftab, Peter Swire, Governor James Gilmore, David Sobel, Stewart Baker, and Jerry Berman. The panels focused on the public's expectations of privacy regarding the government's use of personally identifiable information. The panelists provided diverse points of view and gave the Committee a clear understanding of its upcoming challenges.

A session of public commentary followed in which many speakers echoed their support for the committee. The meeting concluded with a roadmap for future committee action regarding delivering tangible advice to DHS. ⌘

Privacy Office Events

July 14, 2005

Nuala O'Connor Kelly, Speaker (RFID Security Panel) AeA Secure ID, Washington, D.C.
Elizabeth Withnell and Nuala O'Connor Kelly, DHS Internal Data Integrity Board Meeting

August 5, 2005

Department of Homeland Security RFID Summit, Washington, D.C.

September 13-16, 2005

Nuala O'Connor Kelly, Maureen Cooney, & John Kropf,
International Conference on Privacy and Personal Data Protection
Montreux, Switzerland

September 20-22, 2005

United States-European Union Joint Review of the Implementation of the CBP Passenger Name Records Undertakings, Washington, D.C.

September 21, 2005

Kenneth P. Mortensen, Biometric Consortium Conference 2005, Crystal City, Virginia

Upcoming Privacy Workshop

The Privacy Office will host a public workshop this fall to explore public sector use of private sector data and database technologies to aid in the mission of the Department of Homeland Security.

The workshop will explore the government's use of private sector data containing personal information and the privacy implications raised by such use, as well as the developing technologies for analyzing personal information for homeland security purposes. The programs will include leading experts in information policy and technology fields, including representatives of the information industry and the government, to discuss the current use of private sector data and database technologies.

The workshop is scheduled for the week of September 5th. For more information, visit: **www.dhs.gov/privacy**.

Outreach to Europe

Continued from front page

among others.

Kelly also discussed the challenges and opportunities regarding privacy protection, saying, "We have moved from a 'need to know' environment to what is termed as a 'need to share' environment. This can present significant improvements in intelligence information sharing, but also significant challenges to individual expectations for privacy and to institutional privacy safeguards." In confronting the challenges of increased information sharing, Kelly highlighted the need "to establish and enforce concrete safeguards that prevent government from exceeding its proper bounds" through "stronger, more embedded privacy protections." These privacy protections, Kelly said, "must be in place on the front end of our governmental processes, when programs are in their infancy, rather than later and after privacy abuses have occurred."

Kelly underscored the DHS Privacy Office's international efforts noting that, last year, the DHS Privacy Office, as the first statutorily created privacy office in the U.S. federal government, participated in the closed sessions during the International Data Protection and Privacy Commissioners Conference, and will be doing so again this year. "We have worked hard in our office to join the international conversation about both data protection and security," she said.

Kelly's and Cooney's Ireland outreach also included discussions with Permanent Secretary General of the Ministry of Justice Charles Deguara and Data Protection Commissioner Joseph Meade, recently appointed as first Financial Services Ombudsman.

The DHS Privacy Office's efforts at international collaboration on privacy and security continued with John Kropf, Director of International Privacy Programs, attending the third meeting of the Policy Dialogue on Border and Transportation Security on May 19, 2005, in Brussels, Belgium.

Kropf provided a preview of the upcoming Joint Review of the U.S.-EU Undertakings concerning the sharing of Passenger Name Records (PNR). He emphasized the importance of privacy in the PNR arrangement. The DHS Privacy Office will be leading the Joint Review of the US-EU PNR Undertakings.

Immediately following the Policy Dialogue meeting, Kropf participated in meetings of the Working Party on Information Security and Privacy (WPISP) within the Organization for Economic Cooperation Development (OECD) on May 20, in Paris, France. Kropf presented, on behalf of the U.S. delegation and the department, information regarding EITS, to improve verification of travel documents and the identity of travelers. An OECD Experts Group, including Maureen Cooney, Chief of Staff and Senior Advisor for International Privacy Policy at the DHS Privacy Office, is contributing privacy policy guidance on the development of this proposed international information sharing program, in collaboration with technical guidance from the International Civil Aviation Organization (ICAO). Currently, a bilateral pilot is being developed with participation from the U.S., Australia, and the United Kingdom. Kropf provided OECD WPISP members with a report on the pilot project that included a paper to the OECD Experts Group from the pilot project subgroup on Privacy and Legal implications, chaired by Peter Sand, Director of Privacy Technology for the DHS Privacy Office. ⌘

Freedom of Information Act 2004 Annual Report Released

DHS FOIA Annual Report Reveals Accomplishments; Challenges Still Remain

"Through the enormous dedication and hard work across the Department by 340 full-time FOIA staff, with the assistance of 128 program employees, more than 152,000 FOIA and Privacy Act requests were processed in fiscal year 2004," said Nuala O'Connor Kelly, the Chief Privacy Officer for the Department of Homeland Security. "Much of the public interest in understanding the programs and operations of the department is being met by providing access to the department documents through a well managed FOIA program."

The number of requests processed by the department is only 700 requests fewer than the combined total for the Department of Defense, the Treasury Department, and the Department of Transportation. Equally remarkable was that 99.4% of all requests received at least a partial release; only 0.6% of requests were precluded by FOIA exemptions from receiving any release. Of the responses, 33% received a full release; 40% a partial release; 12% had no responsive records, records were not under DHS control, or requests were referred to another federal agency; and 15% were not processed due to withdrawal of request and other reasons, such as the public availability of the documents requested.

The median response times for simple requests by agency ranged from 19 to 84 days, complex requests ranged from 5 to 111 days, and expedited requests ranged from 3 to 45 days.

Every component began fiscal year 2005 with a backlog of requests. The overall backlog for the Department increased by 58%; from 29,000 at the end of fiscal year 2003 to 46,000 at the end of fiscal year 2004. Due to various factors, by the end of FY 2004 the overall number of requests processed decreased almost 6%.

"Factors influencing an increasing backlog," said Tony Kendrick, the Director of Departmental Disclosure and FOIA, "are reflected by a 4% increase in the number of requests received in fiscal year 2004, the complexity and broad scope of requests being received, increasing operational workloads of program staff competing with time available to absorb additional FOIA search workload, a diversity of incompatible FOIA tracking and processing programs, and a changing knowledge-base of FOIA processors due to turnover of processing staff."

"It is our intention to decrease the backlog through a combination of initiatives," said Kelly. "We are moving forward in evaluating a department-wide computerized FOIA and Privacy Act processing system, updating the DHS FOIA implementing regulations to streamline and clarify FOIA responsibilities and accountability throughout the department, and clarifying organizational structures that would include FOIA Officer and Privacy Officer functions and responsibilities at each component and designated special program."

The DHS's Fiscal Year 2004 Freedom of Information Act and Privacy Act Annual Report is available on the Privacy Office website at: www.dhs.gov/foia in the electronic reading room.⌘

Privacy Impact Assessments: Why & When

PIAs Offer Path to Perfecting Privacy Within Department

The e-Government Act of 2002 and the Homeland Security Act of 2002 both require DHS and its components to conduct Privacy Impact Assessments (PIAs) on any new or changing information programs to ensure adherence to privacy protections. In just a brief time, the PIA has become an important part of the process establishing information programs, in terms of both development and legitimacy.

Part development document and part public transparency document, the PIA provides focus for system designers and program managers. It aids system designers in incorporating privacy practices from the outset of the system development cycle, while demonstrating to the public that the system incorporates privacy into the very fabric of its design.

System and project managers often ask the Privacy Office, "Exactly when should we do a PIA?" The short answer is "early and often" throughout the design process. PIAs should be done early because each and every system or program must assimilate privacy protection as a standard feature, and because the PIA is meant to be an organic document, changing as the system does.

A longer answer would be that a PIA should be done when:

1) developing or procuring any new technologies or systems that handle or collect personal information;
2) developing system revisions. If an organization modifies an existing system, a PIA will be required; and
3) issuing new or updated rulemaking that affects personal information. If an organization decides to collect new information or update its existing collections as part of a rulemaking procedure, a PIA is required. Note that the PIA must discuss how the management of these new collections ensures conformity with privacy law.

It is important to note that a PIA is required for all budget submissions to the OMB. In addition, the PIA should show that privacy was considered from the beginning stage of system development.

Following these basic guidelines should help system developers and program managers not only be compliant with the law, but develop a trust with the public--a trust that the government is treating their information fairly and privately.

Of course, there is no need to wonder about the answers to privacy questions, just call the DHS Privacy Office and speak with us about the system concept and initial design. The Privacy Office's Privacy Technology Group is ready to assist in any Departmental development of PIAs.⌘

Meet the Expanding Privacy Office Staff

Toby Milgrom Levin

Privacy Expertise Continues to Build with Addition of Senior Advisor

Toby Milgrom Levin joined the DHS Privacy Office as Senior Advisor with wide-ranging responsibilities, including advising the Chief Privacy Officer on internal and external privacy matters, conducting reviews of possible privacy violations, and coordinating public forums on pressing privacy issues.

Before joining the Privacy Office in April 2005, she was a Senior Attorney in the Division of Financial Practices at the Federal Trade Commission (FTC), where she had worked on privacy matters since 1994. At the FTC, Levin was responsible for numerous privacy projects including bringing the first FTC privacy cases, coordinating public workshops, co-authoring the first FTC privacy reports, and serving as the first manager of the Children's Online Privacy Protection Act enforcement program.

More recently, Levin was one of the FTC's lead attorneys enforcing the Gramm-Leach-Bliley (GLB) Safeguards Rule and coordinating an interagency GLB Notices Project to conduct research to make GLB notices more understandable for consumers.

Levin began her privacy career in the late 1970s as Assistant Director of the National Commission on Confidentiality of Health Records, a non-profit group that grew out of the 1977 Privacy Protection Study Commission Report raising concerns about medical privacy. She joined the FTC in 1984, first working in the Division of Advertising Practices before moving to the Financial Practices Division in 2001.⌘

John Kropf

Privacy Office Adds New Director of International Privacy Programs

John W. Kropf serves as the new Director of International Privacy Programs in the DHS Privacy Office, collaborating with Maureen Cooney, Chief of Staff and Senior Advisor for International Privacy Policy. Kropf is responsible for international program development and advises on international privacy frameworks. His responsibilities include monitoring DHS Security activities for their possible impact on international privacy issues and regulations. He also monitors the department's compliance with international agreements such as the U.S. – EU Passenger Name Records Undertakings and Agreement, which sets guidelines on the collection and handling of passenger data.

As part of his duties, Kropf represents the interests of the DHS at international meetings and as a delegate to multilateral and multinational organizations such as the Organization of Economic Cooperation and Development and the Asian Pacific Economic Cooperation forum. In addition, he engages in bilateral dialogues with representatives of foreign governments and data protection commissions.

Before joining the department, Kropf worked for more than ten years as an international lawyer with the U.S. Department of State in the Office of the Legal Adviser. He has also published on the privacy rights of non-U.S. citizens under U.S. law. He also served two years with the American Embassy in Turkmenistan where he was responsible for USAID programs.

Kropf began his legal career with the U.S. Department of Justice Honors program at the Board of Immigration Appeals and later worked on U.S. claims against foreign governments.

Kropf earned his law degree and a Masters of Public and International Affairs from the University of Pittsburgh. He is a member of bars of Pennsylvania and the District of Columbia.⌘

Lane Raffray

Privacy Office Adds Policy Analyst

Lane A. Raffray recently joined the DHS Privacy Office as a Policy Analyst. In this position, he is responsible for assisting in privacy reviews, evaluating and analyzing policy proposals regarding homeland security privacy matters, and organizing the Privacy Office private sector coordination efforts.

Raffray brings to the DHS Privacy Office a diversity of experience from a public service career spanning local, state, and federal government organizations. Before joining the DHS Privacy Office in March 2005, Raffray served as a 72 Hour Field Coordinator with the Republican National Committee Victory'04 effort in Cuyahoga County, Ohio. He was responsible for the countywide organization of grassroots activities in support of the Bush/Cheney'04 campaign. Prior to the 2004 campaign, Raffray enjoyed a public service career at all levels of government, highlighted by a term as a Research Specialist with the Texas Criminal Justice Policy Council, where he was responsible for conducting criminal justice research and preparing impact analyses on proposed legislation for the Governor and the Texas Legislature. Before joining the state of Texas, Raffray served the state of Tennessee as a Community Planner responsible for administering planning programs for a number of communities in Southeastern Tennessee.

Raffray earned his Master of Public Administration degree from Southwest Texas State University in San Marcos, Texas.⌘

Privacy Advisory Committee Rolls Up Its Sleeves

Second Public Meeting of the DHS Data Privacy and Integrity Advisory Committee Starts Substantive Process to Provide Insight and Information on Privacy to the Department

CAMBRIDGE, Mass. – On June 15, 2005, the Department of Homeland Security (DHS) Data Privacy and Integrity Advisory Committee held its second quarterly public meeting at the Berkman Center for Internet and Society at Harvard Law School. Paul Rosenzweig, the Committee Chair, opened the meeting with a declaration of the Committee's goals and an announcement of the newly formed subcommittees.

Speaking about the committee's goals, Rosenzweig stated that, "We see our initial short-term goal as helping ourselves and the public get a better sense of what the issues are, inventorying the issues at DHS, and identifying where the open privacy questions are." The committee plans to provide written reports to the Secretary of DHS, Michael Chertoff, and the department's Chief Privacy Officer, Nuala O'Connor Kelly, which will include the committee's recommendations regarding how to improve data privacy and integrity in existing and developing DHS programs.

> *"We see our initial short-term goal as helping ourselves and the public get a better sense of what the issues are, inventorying the issues at DHS, and identifying where the open privacy questions are."*

DHS Leadership Presents to Committee

The morning session began with remarks from John Cohen, the Homeland Security Policy Advisor to Massachusetts Governor Mitt Romney, regarding security issues at the state level. Next, key representatives from DHS discussed screening programs in the department.

Robert M. Jacksta, the Executive Director of Border Security and Facilitation from Customs and Border Protection (CBP), was the first to speak to the Committee. Jacksta explained the challenges of processing 1.1 million air travelers, 65,000 trucks or containers, and 365 vehicles every day, noting the steps CBP takes to ensure privacy. Jacksta's appearance was invaluable to the Committee in understanding CBP's commitment to privacy.

Next, Patty Cogswell, Chief Strategist for US-VISIT, spoke about how the program enhances security for our citizens and visitors, while facilitating legitimate travel and trade across our borders. Cogswell emphasized how US-VISIT has safeguarded privacy in the program through privacy policies, training, and by having a privacy officer dedicated solely to the program.

Justin Oberman, Assistant Administrator from Secure Flight and Registered Traveler, addressed the committee, discussing the importance of privacy in these programs. Hard at work in the midst of the Secure Flight screening program development, Oberman took time to explain the full development and testing process for Secure Flight and Registered Traveler, noting how he worked with various groups, including the DHS Privacy Office, to recognize privacy issues while at the same time analyzing the security threat to the nation.

Privacy Experts Present Positions

The afternoon session consisted of presentations and discussions about screening, data mining, and technology issues from an array of technology and privacy experts. The panels included business sector representatives, computer science and privacy experts, and delegates from privacy and technology organizations such as the Center for Democracy and Technology, the American Civil Liberties Union and the Berkman Center. Among those participating in the afternoon session panels were Drs. Simson Garfinkel and LaTanya Sweeney, Daniel Weitzner, Norman Willox, Ari Schwartz, Barry Steinhardt, and Jonathan Zittrain.

Both the morning and afternoon sessions concluded with a public comment period, providing additional perspectives for the committee to consider and integrate into its deliberations.

Site Visits

The day prior to the meeting, the committee had the unique opportunity to participate in site visits to witness and discuss homeland security operations in Boston. The committee members repeatedly expressed their interest in gaining an in-depth understanding of DHS programs and operations with privacy implications during these site visits.

The site visits began with a trip to the Port of Boston Black Falcon Cruise Ship Terminal, where committee members met with U.S. Coast Guard officials, including Captain of the Port Jim McDonald, Joseph Lawless from the Massachusetts Port Authority, and Gary Kijik, a CBP Officer involved in screening cruise ship pas-

See JUNE page 6

Committee Leadership Takes Shape: Balanced Effective Leadership Will Ensure Best Results and Advice for Department

WASHINGTON, DC (April 6, 2005)—At the first meeting of the Data Privacy and Integrity Advisory Committee, Paul Rosenzweig and Lisa Sotto were elected to the positions of Chairman and Vice Chairman, respectively.

Upon announcing their elections, Nuala O'Connor Kelly, Chief Privacy Officer for DHS, noted that the pair brought a balance of points-of-view to the Committee.

"I think they would bring viewpoints that are both divergent but also thoughtful, critical, and respectful of the work of the Department," Kelly said. Both Rosenzweig and Sotto took time to recognize the important role of the committee in helping DHS ensure security without diluting the freedoms so essential to this nation and pledged their efforts for success.

"There is a series of challenges facing the department and more broadly the country in trying to both assess new technologies as they come on line, and their effect on essential liberties that Americans cherish deeply," noted Rosenzweig in accepting his position.⌘

Privacy Office Staff

Nuala O'Connor Kelly
Chief Privacy Officer
Maureen Cooney
Chief of Staff and
Senior Advisor, International Privacy
Sandra L. Hawkins
Administrative Officer
Elizabeth Withnell
Chief Counsel to the Privacy Office
Toby Milgrom Levin
Senior Advisor
Tony Kendrick
Director, Departmental Disclosure
John Kropf
Director, International Privacy Programs
Rebecca Richards
Director, Privacy Compliance
Peter Sand
Director, Privacy Technology
Catherine Papoi
Deputy Director, Departmental Disclosure
Lane Raffray
Privacy Policy Analyst
Kenneth P. Mortensen
Senior Privacy Advisor
Anna Slomovic
Senior Privacy Analyst
Nathan Coleman
Privacy Analyst
Robyn Kaplan
Privacy Analyst
Sandra Debnam
Administrative Assistant
Doug McComb
FOIA Specialist
Sarah Mehlhaff
FOIA Specialist
Dan Stein
FOIA Specialist
Nusrat Rahman
Intern
Katie Smith
Intern
Maria Van Etten
Intern
Collin Jackson
Intern

Component Privacy Officers

Lisa Dean
Privacy Officer, TSA
Elizabeth Gaffin
Privacy Officer, CIS
Andy Purdy
Privacy Officer, IAIP NCSD
Steve Yonkers
Privacy Officer, US-VISIT

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

June Meeting

Continued from previous page

sengers.

During the visit to the Port of Boston, the committee members learned about the challenges of port security, and about how DHS components' work together in their common mission to secure the homeland.

The site visits continued with a trip to Logan International Airport, which consisted of an exceptionally informative tour of CBP operations. With the gracious welcome and assistance of CBP's Boston Field Office, the committee learned about primary inspection procedures for international travelers, including a demonstration of US-VISIT processing, and visited with both the Passenger Analysis Unit and the Counter-Terrorist Response Team. These visits served as invaluable learning experiences for committee members, as the committee begins to examine the department and offer guidance on programmatic, policy, operational, and technological issues within the department that affect privacy.

Advisory Committee Subcommittees Announced

Additionally, since the inaugural meeting, the Committee decided to establish subcommittees to reflect its areas of emphasis. The four subcommittees are: 1) Framework/Principles; 2) Screening; 3) Data Sharing and Usage; and 4) Emerging Applications.

The Framework/Principles Subcommittee will develop guiding principles for the other subcommittees to follow when analyzing DHS programs. Meanwhile, the Screening subcommittee will review current DHS screening policies, technologies, and operations to determine how best to integrate privacy into these programs. The Data Sharing and Usage subcommittee will focus on internal and external data sharing and information exchange. Lastly, the Emerging Applications subcommittee will investigate new technologies, including both those being researched by DHS, as well as technologies from the private sector and academia.

Each subcommittee will issue reports to the full committee for discussion and deliberation.

Future Advisory Committee Meetings

The committee will have two more quarterly meetings in 2005. On September 28, 2005, the committee will meet in Vancouver, Canada to examine border issues and technologies. The committee will meet thereafter on December 6, 2005, in Washington, DC.

For more information about the Data Privacy and Integrity Advisory Committee, visit www.dhs.gov/privacy.⌘

Upcoming Committee Meetings

September 28, 2005
Vancouver, British Columbia

The Data Privacy and Integrity Advisory Committee will be meeting in Vancouver, British Columbia, Canada. The Committee meeting is tentatively set to consider border issues and technology.

Site visits are scheduled for September 27th, in Blaine, Washington, to review technology and screening at the Port of Entry.

December 6, 2005
Washington, D.C.

The December quarterly meeting of the Data Privacy and Integrity Advisory Committee meeting will be held in Washington, DC.

For details as they become available, visit: www.dhs.gov/privacy and click on the link for the Data Privacy and Integrity Advisory Committee.

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. Or 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.