The Privacy Office

Homeland Security

Privacy Matters

Chief Privacy Officer's Message

The Privacy Office remains committed to building a culture of privacy at DHS and as these pages will demonstrate, we have been as busy as ever working on this goal. We have brought our privacy message to Capitol Hill, conducted outreach efforts with our DHS colleagues and the public through our workshops, and reached out to our partners internationally. We do not carry out our work in a vacuum, though, but rather, in partnership across DHS, integrating privacy attentiveness into the Department's mission.

One of our significant achievements was the release of our Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties, otherwise known as the No Fly Report. As required by Section 4012(b)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004, the report provides recommendations to minimize any adverse effects of such lists on privacy and civil liberties. It also reviews the application of those lists to other modes of transportation and discusses how the recommendations would affect such lists' use to protect the U.S. against terrorist attacks. The report was a collaborative effort, reflecting input received internally and externally from our agency partners, and I want to thank everyone who helped on this report, including Toby Levin, Liz Withnell, and former colleague Anna Slomovic.

-Maureen Cooney, Acting Chief Privacy Officer

Inside This Issue, Spring 2006

Secretary Chertoff Opens Committee Meeting

Offers Thanks, Talks Privacy With Privacy Advisory Committee

WASHINGTON, DC (March 7, 2006)— Department of Homeland Security Secretary Michael Chertoff thanked members of the Department's Data Privacy and Integrity Advisory Committee for their efforts and advice and discussed a range of privacy related topics in his remarks opening the first quarterly meeting of this, the Committee's second year in existence.

Calling the DHS environment "probably one of the most challenging in government" with regard to addressing privacy concerns, Chertoff thanked Acting Chief Privacy Officer Maureen Cooney for her "tremendous leadership", calling the Privacy Office's work, "significant."

Chertoff discussed the challenge of defining privacy, noting that the different dimensions of privacy may clash. Still, Chertoff said, the Department remains committed to an information sharing environment.

He expressed a hope that working with the Privacy Office, the Committee would

See CHERTOFF, page 2

Need Help Doing PIAs for OMB-300 or C & A Processes?

Contact us at:

www.dhs.gov/privacy,

Or on email at:

pia@dhs.gov

The Privacy Office Visits Capitol Hill

Acting Chief Privacy Officer Cooney Testifies Before House Subcommittees

WASHINGTON, DC – The DHS Privacy Office returned to Capitol Hill, promoting the Department's privacy efforts during testimony at three Congressional hearings this spring.

On April 4th, the U.S. House of Representatives Judiciary Committee Subcomittee on Commercial and Administrative Law, along with the Subcommittee on the Constitution, convened a joint hearing on Federal government use of personal information supplied by commercial information resellers. In her testimony, Acting Chief Privacy Officer Maureen Cooney told the committee that DHS uses privacy impact assessments (PIAs) as a tool to address privacy questions at the outset of an information project. Furthermore, Cooney said, "It is DHS policy that any time data from an information reseller is used in a decision-making process, whether the decision involves correcting existing information or obtaining new information, a PIA is required."

Cooney also highlighted for the subcommittee the role of the DHS Privacy Office as a leader in the dialogue on the use of commercial data, both within and outside the Department, citing its sponsorship of *Privacy and Technology: Exploring the Use of Commercial Data for Homeland Security*, a public workshop held in September 2005. "With input from the public workshop, the DHS Privacy Office is now in the process of drafting

See HILL, page 2

Chertoff Opens Advisory Committee Meeting— Continued

help build into DHS a "respect for privacy," and "a thoughtful approach to privacy."

"We want the government to be a protector of privacy, and we want to build security regimes that maximize privacy protection and that also do it in a thoughtful and intelligent way," he said.

Closing his remarks, the Secretary stressed to the Committee its role in creating a culture of privacy at DHS, a culture that, if done correctly, " will be not only a long-lasting ingredient of what we do in Homeland Security, but a very good template for what government ought to do in general when it comes to protecting people's personal autonomy and privacy."

The complete text of Secretary Chertoff's remarks can be found at: http://www.dhs.gov/dhspublic/display?content=5481.

For more on the DHS Data Privacy and Integrity Advisory Committee meeting on March 7th, see page 5.⌘

Privacy Office Events

June 7, 2006

Data Privacy and Integrity Advisory Committee Meeting; San Francisco, CA

June 15, 2006

Department of Homeland Security Privacy Office Workshop: Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments; Washington, DC

June 21, 2006

Maureen Cooney, Keynote Speaker, Enterprise Rights Management Conference: Data Privacy & Security, Silver Spring, MD

July 19, 2006

Maureen Cooney, Keynote Speaker, IT Security Magazine's "Best Practices for Defending Against Insider Threat to Proprietary Data Conference"; Arlington, VA

August 21-25, 2006

Department of Homeland Security: Security Conference & Workshop; Baltimore, MD

Privacy Workshop: Compliance & PIAs

The DHS Privacy Office continues its popular workshop series with a workshop entitled, "*Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments.*" The event will explore the policy and operational frameworks required to integrate privacy protections into any organization. The workshop may be particularly valuable, as it coincides with the annual OMB-300 budgeting process and the ongoing Certification and Accreditation process under the Federal Information Management Security Act, both of which require programs to conduct PIAs.

The workshop will be organized into two sessions. The morning session will include two panels. The first will focus on how entities can operationalize privacy and the second on how agencies comply with Federal requirements for privacy. The afternoon session will be a tutorial on writing PIAs and Privacy Threshold Analyses. For more information, visit: www.dhs.gov/privacy. ⌘

Privacy Office On the Hill — Continued

specific guidance on the use of commercial data for homeland security purposes," Cooney added. This guidance will address comparing data in commercial and government databases, obtaining commercial data for use in government systems, and the use of government analytic tools on commercial databases. Cooney also told the subcommittee that, in October 2005, the DHS Data Privacy and Integrity Advisory Committee presented to Secretary Chertoff a report on the use of commercial data in passenger screening programs to reduce false positives.

While there may be many benefits from government's responsible use of commercial data, Cooney asserted that such use "must be transparent and appropriate." Commercial data, she said, must be "used responsibily and with respect for individuals' legitimate expectations of privacy."

On April 6th, Cooney again testified on the Hill, this time before the House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, which convened a public hearing on the protection of privacy within DHS's Intelligence Enterprise.

"Privacy is a cultural value at DHS," Cooney told the subcommittee. "We want the government to be a protector of privacy," she said, echoing the sentiments expressed by Secretary Chertoff last March.

Cooney underscored for the subcommittee the means the Privacy Office uses to embed sound privacy practices, as well as accountability and transparency, into DHS systems, including Privacy Act notices, PIAs, privacy audits, and complaint reviews.

Furthermore, Cooney noted that while the E-Government Act may exempt national security systems from PIA requirements, the Privacy Office requires all DHS systems –including national security systems –to complete a PIA if they contain personal information. Cooney testified that this policy ensures that privacy considerations are integrated into the information systems which are part of the DHS Intelligence Enterprise.

Regarding information sharing, Cooney said, "The Privacy Office policy supports the exchange of information between the Department's component organizations whenever those organizations establish an appropriate need based on an express purpose."

On May 17th, Cooney again appeared before the House Judiciary Subcommittee on Commercial and Administrative Law to testify about the role of the DHS Privacy Officer at a hearing on "Privacy in the Hands of the Government."

Stressing its PIA guidance, which has become a model in the Federal government; privacy compliance reviews; privacy education and training; and international and other outreach efforts, Cooney said the Privacy Office "has worked to enhance public trust in the Department and to ensure the protection" of the privacy interests of American citizens and foreign visitors.

For the text of DHS Privacy Office testimony, visit: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0510.xml⌘

Cooney Heads US Team at APEC Privacy Meeting

Information Privacy in E-Government & E-Commerce, APEC Framework Discussed in Hanoi, Vietnam

HANOI, Vietnam—On February 20-24, Acting Chief Privacy Officer Maureen Cooney presented at the Asian-Pacific Economic Cooperation (APEC) Symposium on Information Privacy in E-Government and E-Commerce, joining officials and private sector representatives from more than twenty APEC member countries, and led the U.S. delegation at the APEC E-Commerce Working Group meeting.

In addition to Cooney, the U.S. delegation included Martin Abrams of Hunton and Williams, Markus Heyder of the Federal Trade Commission, Eric Holloway of the Department of Commerce, Julie Inman of Microsoft-Asia/Pacific, Michael Lewis of Warner Bros. Online, James Reynolds of the Department of Justice, Heather Shaw of the U.S. Council for International Business, and Patty Sefcik of the Department of Commerce, who chaired the meeting of the APEC E-Commerce Working Group.

Cooney's presentation included a variety of subjects, including an introduction to the DHS Privacy Office, an overview of the U.S. privacy framework, and current international issues confronting DHS, including lost or stolen passports, Passenger Name Record accords, the use of biometric identifiers, and U.S. data sharing agreements, and the continuing focus of the DHS Privacy Office to operationalize privacy through privacy impact assessments.

Cooney also discussed the APEC privacy framework, noting the importance of the framework's focus on preventing harm to individuals through the identification and mitigation of privacy and security risks. Cooney noted flexibility and consensus as a strength of the framework; it was founded on the principle of reducing barriers to information exchange while maintaining privacy. Cooney noted other strengths of the framework as well, stressing its consistency with the OECD guidelines on trans-border flows issued in 1980, and its flexibility for both public and private entities.

Cooney stressed privacy impact assessments to measure the privacy risks associated with techologies, communicate privacy protections, and improve how government and business handles consumer information.

Implementation of the framework is believed to be an important step toward facilitating appropriate cross-border information exchange, such as the current project between DHS and APEC countries involving the real-time exchange of data on lost or stolen passports.⌘

Privacy Office Leads ID Theft Discussion for International Audience

First European Data Protection Congress in Madrid, Spain, Highlights Plethora of Privacy Perspectives

MADRID, Spain—On March 29-31, the Spanish Data Protection Agency, in conjunction with the BBVA Foundation, hosted the first European Data Protection Congress. John Kropf, Director of International Privacy Programs for the DHS Privacy Office, joined over 100 participants from Europe, Mexico and the United States who offered presentations on a wide-ranging program including the technical, legal, social and philosophical aspects of biometrics.

Kropf participated in a panel discussion: *The Fight against Fraud and Data Protection*. Kropf emphasized a specific fraudulent use of personal information, namely identity theft. Kropf's presentation included an overview of pending legislation at the state and Federal levels, a discussion of the REAL ID Act, a description of the U.S. Inter-Agency Community's outreach on ID theft, and an overview of international developments.

Kropf underscored for the audience that the identity theft issue has the attention of lawmakers at all levels of government in the United States. His review included proposed Federal legislation to limit the misuse of social security numbers; a bill to require Federal agencies possessing personal information to disclose data breaches; and a bill to prevent and mitigate ID theft, ensure privacy, provide notice for security breaches, and enhance criminal penalties for misuse of personal information.

At the state level, Kropf told the Congress that some 20 states have legislation, either in force or proposed, to address the issue of ID theft. Specifically, he mentioned the "ID Theft Passport" idea proposed in Iowa, which would create a document for victims of ID theft to show creditors and police. Also noted was a new Wisconsin law requiring notifying consumers if their personal information is stolen and proposed California legislation to strengthen criminal penalties for the theft, sale or misuse of personal information.

As for REAL ID, the Federal law requiring state driver's licenses and ID cards to meet certain standards if they are to be accepted by the Federal government for official purposes, Kropf said, "DHS has primary responsibility for developing implementing regulations. The [DHS] Privacy Office is leading Federal efforts to ensure that the regulations incorporate strong privacy protections." He also noted the cooperation of the Department of Transportation and other agencies in this effort.

In addition, several agencies across the Federal government have ID theft enforcement and outreach programs, including the Social Security Administration, Department of the Treasury, Department of Education, Federal Deposit Insurance Corporation, Federal Reserve Board, National Credit Union Administration, and the Department of Health and Human Services.

Kropf noted that the problem of lost or stolen passports has raised concerns over ID theft internationally, as over nine million passports have been lost or stolen. However, according to Kropf, international data sharing can make a significant contribution to preventing ID theft schemes that rely on fraudulent travel documents.

The discussion turned to the U.S. government's efforts at international data sharing, including an agreement with Australia and New Zealand to share information on lost or stolen passports, and the Enhanced International Travel Security (EITS) program for validating international travel documents. The EITS effort, still in the planning phase, is led by the U.S., United Kingdom, and Australia and incorporates advice from privacy experts from the Organization for Economic Cooperation and Development.⌘

Privacy Office Continues Public Workshop Series

Government Accountability & Transparency Session Attracts Large Audience

WASHINGTON, DC— On April 5, 2006, the Department of Homeland Security (DHS) Privacy Office hosted its second public workshop, "*Transparency and Accountability: The Use of Personal Information within the Government.*" The workshop explored comparative government frameworks regarding transparency and accountability, focusing on public notices and freedom of information frameworks. A large audience, including representatives from both government and the private sector, attended the workshop. A large delegation of international government officials from Europe, Japan, Canada and Mexico, including members of the International Working Group on Data Protection in Telecommunications ("the Berlin Group") also attended.

The workshop opened with a panel discussion of how privacy notices are used as a tool for transparency. Highlights of the panel included a discussion, featuring two government representatives from the Department of the Treasury and the Federal Trade Commission, on a consumer research study conducted by their agencies, as well as several other federal agencies, the goal of which was to improve financial notices to consumers. The research endorsed the use of short, layered privacy notices In addition, European officials discussed the complexity of privacy notices and what is being done to make them clearer.

The next panel addressed the balance between privacy of personal information and the public interest. The panelists focused their discussion on Freedom of Information Act (FOIA) requests, and in particular, two of the nine statutory exceptions that a U.S. government agency may elect in order to withhold information to protect an individual's privacy. One exception is unique to law enforcement records and the other applies to other federal records that contain information about an individual. Many of the panelists shared stories from their experiences in government where these particular exemptions were exercised. Additionally, there were panelists representing FOIA from the requestor's point of view. They spoke about some of the redress and appeals available to those denied information under the FOIA.

In the afternoon María Marván, President of the Mexican Access to Information Institute, spoke about Mexico's recent passage of an access to information law. In 2000, after 70 years of one ruling party, a new party won the Presidency. In 2002, the Mexican Congress unanimously approved the first Freedom of Information Act. Since then all but four Mexican states have enacted privacy laws.

The workshop concluded with an international panel discussion comparing how the governments of different nations provide access to information while protecting the privacy of individuals. The governments of the U.S., Germany, Canada, the United Kingdom and Mexico were represented on the panel. Panelists discussed how first– and third-party information requests are handled in their respective countries.

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

Certification & Accreditation Process Aids PIA Program

Interdepartmental Cooperation Highlights Compliance Process, Fosters Culture of Privacy

Privacy Impact Assessments (PIAs) are a key aspect of the Department of Homeland Security's privacy compliance efforts. The Privacy Office coordinates the completion of PIAs for the Department and its components. Although the program office and/or system owners are responsible for drafting PIAs, the Director of Privacy Compliance, in coordination with the Privacy Office's Chief Counsel, ensures that the Department's PIAs contain substantive responses which satisfy legal, regulatory, and policy requirements, and that PIAs are completed in a timely fashion. The Chief Privacy Officer approves all PIAs for the Department and its components.

In addition to working with the Chief Information Officer (CIO) and the Chief Financial Officer on the Enterprise Architecture Center of Excellence, and the Office of Management and Budget (OMB) investment review process, most recently, the Privacy Office has begun using the Chief Information Security Officer (CISO) Trusted Agent FISMA tool to track the progress of PIAs as part of the Certification and Accreditation (C & A) process. The C & A process is designed to ensure that each Department system meets technical and security standards as enforced by the CIO and Chief Information Security Officer. As part of compliance reporting requirements to OMB, the C & A process requires either completion of a PIA or the determination that a PIA is not necessary.

The Privacy Office reviews the privacy documentation for each system undergoing C & A review. At a minimum each system is required to submit a Privacy Threshold Analysis (PTA). The PTA outlines general information about a system, including the year the system was developed, a description of the system, and what personal information the system collects or uses, if any. After review and possible dialogue with the information security officer or program manager responsible for privacy issues, the Director of Compliance determines whether a PIA is needed.

If no PIA is necessary, the PTA is sufficient as privacy documentation, and the system may move forward having satisfied the privacy elements of the C & A process. If a PIA is necessary the system owner or person responsible for privacy issues is given the Department's PIA guidance and a PIA template, which is designed for simplicity of use and the control of forms.

The C & A process is important to the Privacy Office's PIA program because it allows the office to monitor new and developing systems and to develop working relationships with program managers, system owners, and information security officers working all over the country and within the Department. The Privacy Office works closely with the Office of the Chief Information Officer and values its relationship with the information policy and information security offices.

Based on feedback from the program and system owners as well as from DHS senior leadership, the Privacy Office will continue to further refine the C & A process as it pertains to privacy issues. Ensuring complete compliance on privacy issues is a goal of both the Privacy Office and DHS as a whole.⌘

Data Privacy and Integrity Advisory Committee Begins Second Year

Secretary Chertoff's Remarks and Framework Report Highlight Recent Committee Meeting

WASHINGTON, DC— On March 7, 2006, the DHS Data Privacy and Integrity Advisory Committee kicked off its second year, hosting its first quarterly meeting of 2006 at the Ronald Reagan Building and International Trade Center in Washington, DC.

Secretary Chertoff Opens Meeting with Remarks

DHS Secretary Michael Chertoff opened by thanking the Committee for its work, specifically mentioning its recommendations about the use of commercial data to reduce false positives in DHS screening programs.

In his remarks, the Secretary noted that privacy "actually means different things to different people." These differences create the challenging environment in which DHS and the Committee both operate.

About information sharing at DHS, Chertoff said, "Clearly, we need to be committed to better information sharing, and the question is, how do we build protocols and regimes to make sure that information is used appropriately and not misused."

Chertoff also stressed privacy in his remarks, noting that because of the relative youth of DHS, there was " a lot of opportunity" to imbue the Department with "a respect for privacy" and a "thoughtful approach to privacy."

"We want government to be a protector of privacy," Chertoff told the audience.

> *"We want the government to be a protector of privacy. . . ."*
> *- DHS Secretary Michael Chertoff*

National Academy of Sciences Study on Privacy Discussed

The Committee welcomed Senior Program Officer Betty Chemers and Senior Scientist Herb Lin to preview a proposed National Academy of Sciences study: *Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*.

The study, which is funded in part by DHS, will address the Federal government's information needs within the challenging context of preventing terrorism. More specifically, the study proposes to examine the connections among terrorism prevention, technology, and privacy.

Chemers told the Committee that the study was just beginning, but that the study committee would be meeting several times over the next 18 months. Chemers said, "There is a real attempt to develop consensus among the [study] committee members." She also stressed the study committee's independence from government, noting that the government does not appoint people to the study committee. Chemers added, "And the government really does not see the report until [it] is completed."

Panels Discuss DHS Information Sharing Environment

The Committee hosted two panels on information sharing, one called: *Building an Information Sharing Environment*, the other entitled: *Operating Within an Information Sharing Environment*.

The information sharing environment panel included Dr. Carter Morris, Director of the Information Sharing and Knowledge Management for DHS Intelligence and Analysis; Al Martinez-Fonts, Assistant Secretary, DHS Private Sector Office; and Chet Lunner, Acting Director, DHS Office of State and Local Government Coordination. Panelists discussed the challenges they face, such as exchanging information between security levels, getting actionable information to the private sector, and increasing preparedness through information sharing with state and local governments.

The panel on operating within an information sharing environment included Jim Williams, Director, DHS US-VISIT; Scott Charbo, DHS Chief Information Officer; Luke McCormack, Chief Information Officer, DHS Immigration and Customs Enforcement (ICE); and Frank DiFalco, Director, Homeland Security Operations Coordination. Panelists discussed current programs, practices, and challenges within an information sharing environment.

Privacy Framework Report Adopted

The Framework subcommittee presented its report: *Framework for Privacy Analysis of Programs, Technologies, and Applications* to the full committee for approval. The report offers a framework for DHS to employ when considering the privacy impacts of "personal data-intensive programs and activities." The five steps of the framework are: scope, legal basis, risk management, effects on privacy interests, and recommendations. The full committee amended, then approved the report.

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

Advisory Committee Welcomes New Chairman: Effective, Balanced, Leadership Continues

WASHINGTON, DC—The leadership of the DHS Data Privacy and Integrity Advisory Committee is set for the coming year. J. Howard Beales, III, will lead the Committee as its Chairman, with Lisa J. Sotto continuing her service as Vice-Chairman.

Beales is an Associate Professor of Strategic Management and Public Policy at The George Washington University. Previously, he served for three years as the Director of Consumer Protection at the Federal Trade Commission, where privacy was a key initiative during his tenure. He is serving a three-year term on the Committee.

Sotto is a Partner at Hunton & Williams in New York. She heads the firm's Regulatory Privacy & Information Management Practice and works extensively with the firm's Center for Information Policy Leadership on topics ranging from improved privacy notices to responsible pattern analysis. She is serving a four-year term on the Committee.

Both Beales and Sotto have served on the Committee since its inception in April 2005, and will serve in their leadership positions through May 2007.⌘

Privacy Office Staff

Maureen Cooney
Acting Chief Privacy Officer &
Chief FOIA Officer

Sandra L. Hawkins
Administrative Officer

Kenneth P. Mortensen
Acting Chief of Staff

Elizabeth Withnell
Chief Counsel to the Privacy Office

Toby Milgrom Levin
Senior Advisor

John Kropf
Director, International Privacy Programs

Peter E. Sand
Director, Privacy Technology

Rebecca Richards
Director, Privacy Compliance

Billy Spears
Director, Privacy Education & Training

Tony Kendrick
Director, Departmental Disclosure & FOIA

Catherine Papoi
Deputy Director, Departmental
Disclosure & FOIA

Erica Perel
Attorney-Advisor

Lane Raffray
Policy Analyst

Cathy Lockwood
Senior Policy Analyst

Nathan Coleman
Privacy Analyst

Kathleen Kavanaugh
Privacy Outreach Coordinator

Tamara Baker
Executive Event Coordinator

Rachel Drucker
PIA Coordinator

Sandra Debnam
Administrative Assistant

Erin Odom
Administrative Assistant

Vania Lockett
Senior FOIA Specialist

Mark Dorgan
FOIA Specialist

Stephanie Kuehn
FOIA Specialist

James Larsen
FOIA Specialist

Shannon Snypp
FOIA Specialist

Andrew Hoffman
International Privacy Programs Intern

Erika Shehan
Privacy Technology Intern

Component Privacy Officers

Steve Yonkers
Privacy Officer, US-VISIT

Peter Pietra
Privacy Officer, TSA

Elizabeth Gaffin
Privacy Officer, CIS

Andy Purdy
Privacy Officer, NCSD

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

Comprehensive Outreach a Priority, Success

Advisory Committee, Training, International, and Hill Visits, Highlights

Since its inception in April 2003, the DHS Privacy Office has worked tirelessly to achieve its mission- to support the Department in its efforts to protect the homeland, while at the same time safeguarding the privacy of individuals, and in particular the individual's personal information. To achieve its mission the Privacy Office works everyday, fostering collaboration with those whom it considers its partners in privacy: its colleagues within the Department, privacy advocates, Members of Congress, citizens at-large, and the international community. As it has for over three years, the Privacy Office continues to strive to communicate its goals, build relationships, and raise privacy awareness through a variety of means, all of which combine to create a comprehensive and inclusive approach to outreach.

Among the most visible of the Privacy Office's outreach tools is its series of public workshops. The series began in September 2005 with a feature exploring the use of commercial data for homeland security. A workshop highlighting transparency and accountability in government followed in April 2006. The public workshop series, which has quickly become very popular among privacy professionals across the Federal government and the private sector, offers privacy practitioners and the public access to a broad range of privacy perspectives and an opportunity for a greater understanding of real-life applications of privacy principles. Next in the series is a workshop on privacy impact assessments and policy coming in June.

The Privacy Office's outreach efforts have an internal focus as well, featuring the development and implementation of a comprehensive privacy training program for new and existing employees and contractors. A privacy awareness training has already been developed, with additional modules to debut by the year's end.

Internationally, the Privacy Office is continuing its outreach, its relationship building, with our partners around the world. Using its outreach tools, along with international forums, the office promotes privacy and security.

The DHS Data Privacy and Integrity Advisory Committee meetings are another valuable outreach mechanism. Comprised of leading privacy experts from private sector, non-profit, and government organizations, the advisory committee advises the Secretary and the Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, data integrity and data interoperability. Held quarterly since April 2005, these interactive public meetings offer a unique opportunity for Privacy Office staff, DHS officials, privacy experts and the public to share a dialogue on current topics of interest within DHS. Over the past year, the advisory committee has welcomed Secretary Chertoff and Deputy Secretary Jackson, as well as many senior-level leaders at DHS and members of Congress, such as the Honorable Chris Cannon (R-UT), Chairman of the Subcommittee on Commercial and Administrative Law of the House Judiciary Committee and the Honorable Bennie Thompson (D-MS), Ranking Member of the House Committee on Homeland Security. The advisory committee meetings have served as a forum for a wide range of cutting-edge topics in homeland security, among them screening programs, radio frequency identification use, and redress programs at DHS; international perspectives on cross-border cooperation and homeland security; state government perspectives on homeland security; and risk-based analysis and its application to DHS. Furthermore, the advisory committee is fulfilling its advisory role, producing reports on commercial data usage by DHS, the Secure Flight program, and a recommended framework to aid DHS in analyzing programs, technologies and applications for privacy related concerns.⌘

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 privacynews@dhs.gov. Please note that topics should be related to privacy or FOIA issues, rather than privacy or FOIA products or services.