

**DHS Data Privacy and Integrity Advisory Committee
Minutes from Public Meeting
November 7, 2012**

Committee members in attendance:

Lisa Sotto, Chair
Craig W. Bennett
James M. Byrne
Renard Francois
Melodie M. Gates
Joanna Grama
David A. Hoffman
Greg Nojeim
Charles Palmer
Christopher Pierson
Tracy Pulito
Barry Steinhardt
Marjorie S. Weinberger

Also in attendance:

Jonathan R. Cantor, Acting Chief Privacy Officer and Sponsor, Privacy Office, Department of Homeland Security (DHS)
Brendan Goode, Director, Network Security Deployment, National Protection & Programs Directorate (NPPD), DHS
Shannon Ballard, Designated Federal Officer, Privacy Office, DHS
Dan Chenok, Chair, DPIAC Cybersecurity Subcommittee (subject matter expert)
Sharon B. Franklin, DPIAC Cybersecurity Subcommittee (subject matter expert)

Chair Lisa Sotto called the meeting to order at 1:05 p.m. and welcomed Committee members and the public to the first Committee meeting of the fiscal year.

DHS Chief Privacy Officer's Update:

Acting Chief Privacy Officer, Jonathan R. Cantor, provided an update on DHS Privacy Office activities since the DPIAC's July 17, 2012 meeting, including accomplishments from the Privacy Policy and Advocacy, International Privacy Policy, Compliance, FOIA and Privacy Oversight Groups.

Annual Report

Mr. Cantor advised that in September, the Privacy Office published its FY2012 Annual Report to Congress, which highlights the accomplishments/activities of the Privacy Office and reports on DHS components' privacy related activities.

Office Move and Staff

Mr. Cantor advised that in August, the Privacy Office relocated from Rosslyn, VA to Massachusetts Ave. NW, Washington, DC, which resulted in significant savings of overhead expenditures. Since the July meeting, one senior staff member began a year-long detail as the

White House National Security Staff Director for Privacy and Civil Liberties and that the office added a new position entitled Director, FOIA Improvement. Three new employees joined the office.

Training

Mr. Cantor advised that PRIV continues to conduct new employee training to address FOIA and safeguarding personally identifiable information (PII). PRIV Chief of Staff continues to provide professional development to office staff.

Privacy Policy and Advocacy

Mr. Cantor advised that Mary Ellen testified in July before the Senate Homeland Security and Governmental Affairs Committee, Subcommittee on Oversight of Government Management, where she focused on the unique statutory authorities of the DHS Chief Privacy Officer and the Department's issuance of a directive on social media.

Mr. Cantor reported that he will testify on November 15 before the House Homeland Security Committee, Subcommittee on Transportation Security to discuss Advanced Imaging Technology.

Fusion Centers

Mr. Cantor discussed the Privacy's Office response to the Senate Permanent Subcommittee on Investigations' report on fusion centers. PRIV participated in the investigation and was interviewed by the Subcommittee. The report noted that the review process that DHS uses for finished intelligence and raw reporting is working and is worthwhile. PRIV will continue to promote privacy training in collaboration with DHS's office for Civil Rights and Civil Liberties.

International Privacy Policy (IPP)

The Privacy Office continues to work closely with the Office of International Affairs and DHS components to implement the Privacy Principles from last year's U.S.-Canada Beyond the Border (BTB) Declaration. In September, DHS began Phase I of the Entry/Exit program outlined in the BTB action plan.

The Privacy Office continues to participate as part of the USG team in negotiating the U.S.-EU "umbrella" agreement (Data Protection and Privacy Agreement), and also contributed to the negotiation of a U.S.-UK visa and immigration information sharing agreement.

Our international team continues to participate with other executive agencies in developing responses to the proposed European Union data protection regulation and directive.

Lastly, the Privacy Office played a leadership role in the interagency development of a USG strategy for the OECD Working Party for Information Security and Privacy.

Compliance

Between July 18 and October 31, 2012, the Privacy Office completed: 188 PTAs, 25 PIAs, six SORNs, and one computer matching agreement.

The Privacy Office reported a Department-wide percentage of 85 percent compliance rate for PIA's and 98 percent compliance rate for SORNs in the Secretary's Annual FISMA report in November, the highest scores ever reported by the Department.

Mr. Cantor outlined four of the key PIA's that the office approved since July, including the Joint Cybersecurity Services Program PIA and the PIA Update for the Western Hemisphere Initiative.

FOIA

DHS sponsored two training events for FOIA professionals, which included a FOIA best practices training with other agencies and a Department of Justice briefing on new guidance on the use of FOIA statutory exclusions. Our Director of FOIA Improvement provided FOIA training to the DHS Office of Health Affairs staff.

Last month, Delores Barber, Deputy Chief FOIA Officer, hosted a FOIA celebration recognizing the contributions of DHS staff throughout the components.

Mr. Cantor then reported that for FY 2012, DHS received over 194,000 FOIA requests and processed over 203,000 requests, while decreasing its backlog to about 28,000 requests. This was a 34 percent decrease of the FOIA backlog.

In September, the Privacy Office launched an electronic FOIA solution, FOIA Xpress, which will be deployed across the department.

Lastly, the FOIA website was updated to be more user friendly.

Privacy Oversight

As discussed during the July meeting, the new strategic plan for PRIV included the consolidation of privacy complaint and privacy incident handling functions, Privacy Compliance Reviews (PCR), and privacy investigations into a new oversight team.

The Oversight team hosted the fourth annual Core Management Group meeting for component staff to discuss privacy incident reporting over the last two years. The panel presented best practices for collaborating to address privacy incidents.

The Oversight team continues to work with component privacy officers to implement the Management Directive addressing the Department's Use of Social Media.

Lastly, Mr. Cantor explained that the PCR's allow staff to see if programs adhere to representations made in PIA's and SORN's.

Following his report, Mr. Cantor responded to questions and comments from the Committee.

Presentation on the National Cybersecurity Protection System

Brendan Goode, Director of Network Security Deployment in DHS's Office of Cybersecurity and Communications (CS&C) provided an overview of the National Cybersecurity Protection System (NCPS). [Mr. Goode's presentation is posted under "meeting" on the DPIAC website.] In 2008, the Comprehensive National Cybersecurity Initiative (CNCI) outlined the strategic plan for Federal cybersecurity. NCPS, which is also referred to as EINSTEIN, is DHS's program of record for satisfying the goals of the CNCI. EINSTEIN focuses on advanced, persistent threats against the federal enterprise and is meant to alert DHS to those types of attacks.

Securing federal civilian networks is a complex challenge that could not be addressed all at one time, so DHS rolled out a series of incremental "block" programs to fulfill the CNCI initiatives. Block 1.0 ("EINSTEIN 1") provided retrospective flow analysis of the connection between federal networks and the internet, analyzing historical cybersecurity incidents. Block 2.0 ("EINSTEIN 2") provides DHS with real time alerts of malicious traffic on federal civilian networks. Block 2.1 improves EINSTEIN 2's analytic capabilities. Block 2.2 provides a secure environment for sharing cybersecurity information at all classification levels. Block 3 ("EINSTEIN 3"), which is targeted for initial implementation in FY 2013, will provide the ability to block active intrusions.

Following Mr. Goode's presentation, DPIAC members were invited to provide comments or questions. Members asked about the DHS Privacy Office's involvement in the process to decide to launch cybersecurity capabilities; the level of automated analytics in the security incident event management system and whether privacy protections had been inserted into the automated analytics; how DHS is addressing the challenge of handling a variety of protections covering information sharing and passing information on to another group that may have different policies in place; whether DHS has all the statutory authority necessary to do its cybersecurity work or whether there are gaps in DHS's authority; and whether DHS plans to develop the capability to identify and go after bad cybersecurity actors.

Subcommittee Reports/Committee Discussion:

Policy Subcommittee

The DPIAC's Policy Subcommittee advised fellow DPIAC members of the status of their report, prepared in response to a tasking from the Chief Privacy Officer for Policy Recommendations on use of Live Data in Research, Testing, or Training.

Chris Pierson, Acting Chair for the Policy Subcommittee, presented the Subcommittee's draft report. He advised that subcommittee members collected information for the report from its members and from information received from several DHS components, including Immigration & Customs Enforcement (ICE), Science & Technology, and US Customs & Immigration Services. He explained that several of DHS's components, such as Customs & Border Patrol and ICE, need to use live data to perform their functions, which include identifying false documents that individuals use to gain entry to our country or otherwise.

He advised that the members concurred that there needs to be a written approval process for CPO's to determine when it is appropriate to use live data. He expounded that the terms live

data and real data must be clearly defined in the process, and that the intake process must be robust and sustainable, like the one that is currently used by ICE.

Mr. Pierson advised that the members reviewed the risk mitigation process and addressed issues such as onward transfer and retention schedules for disposing of data. The report is intended to provide guidance to DHS that is concrete, actionable, and operational.

Lastly, the Chair reported that the subcommittee will meet at the end of November, and that their goal is to finalize their report so that it can be submitted to the full committee by the next DPIAC meeting tentatively scheduled for February 2013.

Cybersecurity Subcommittee (please see transcription on website for full text)

Next, Dan Chenok, Chair of the DPIAC Cybersecurity Subcommittee, gave a presentation of the Subcommittee's findings regarding privacy considerations in departmental cybersecurity pilots. The Subcommittee is composed of DPIAC members and non-DPIAC subject matter experts. All Subcommittee members have appropriate security clearances and have received classified and unclassified briefings from DHS. Mr. Chenok noted that the Subcommittee had numerous classified discussions with DHS on cybersecurity, had reviewed its understanding of those discussions, and had reviewed several reports, including the 2006 DPIAC Framework, to develop its recommendations.

Mr. Chenok explained that the scope of the Subcommittee's report is limited to cybersecurity pilots, such as the types of activities discussed in Mr. Goode's presentation or the JSCP in its early stages. Mr. Chenok noted that the report is not related to one particular pilot but is intended to be helpful guidance for pilots going forward now or in the future. The report is not related to other cybersecurity activities that DHS is involved in.

The Subcommittee had two key findings regarding specific privacy protections DHS should consider when sharing information from a cybersecurity pilot project with other agencies. First, the principal goal of any cybersecurity pilot is to get the right information to the right people at the right time. Consequently, pilots should not over collect or over shared, but should be a targeted program with data minimization and retention policies in place. Second, consistent with the DPIAC's work, the foundation of any pilot should be the DHS Fair Information Practice Principles (FIPPs). Mr. Chenok then reviewed the Subcommittee's key recommendations.

The Subcommittee had two key findings regarding privacy considerations DHS should include in evaluating the effectiveness of cybersecurity pilots. First, DHS documentation for evaluating pilots does not include privacy as an explicit evaluation criterion, so that should be included. Second, groups like the Subcommittee and privacy experts from across DHS should be involved in the design and evaluation of pilots from the beginning.

Members discussed the draft report, made minor additions/edits, and then voted to accept the recommendations as a final DPIAC report. The final report is posted on the website.

Technology Subcommittee (please see transcription on website for full text)

David Hoffman, Chair of the DPIAC Technology Subcommittee, presented the text of the Subcommittee's final recommendations for privacy best practices associated with the department's collection and use of biometrics in response to an April 2012 tasking from the CPO.

In conducting its research, the Subcommittee received briefings on potential uses of biometrics by the Department. Mr. Hoffman clarified that the Subcommittee's report was not a review of any specific program or a gap analysis of any particular implementation, so should not be interpreted as a critique of current DHS privacy practices.

The Subcommittee recommended a four-step analysis for DHS to consider. These steps include:

1. evaluate the usefulness and utility of a biometric method,
2. recognize the potential privacy impacts of biometric use,
3. review program requirements of biometric use, and
4. consider the risks and benefits of deploying biometrics.

The Subcommittee further recommended privacy protections for biometric use for identification purposes and used the 2006 DPIAC framework document to analyze this issue. The DHS Fair Information Practice Principles (FIPPs) were analyzed for its application to biometric collection and use, including transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. This analysis resulted in 15 recommendations.

Members discussed the draft report, made minor additions/edits, and then voted to accept the recommendations as a final DPIAC report. The final report is posted on the website.

Public Comments:

Jeremy Scott, the national security fellow at the Electronic Privacy Information Center, formally address the DPIAC. Mr. Scott recognized the good points made in both the cybersecurity pilot and biometrics reports and their reference to the Privacy Act, but lack of reference to the Freedom of Information Act (FOIA). He encouraged the committee to recommend that DHS not exempt records collected under its programs from Privacy Act provisions and to adhere to the openness requirements of FOIA by further emphasizing transparency and accountability.

Closing Remarks

DPIAC Chair, Lisa Sotto, reminded members of the public that they may submit written comments at any time and to email said comments to privacycommittee@hq.dhs.gov. The meeting was adjourned at 4:20 p.m.