DHS Data Privacy and Integrity Advisory Committee
Public Meeting
September 12, 2013

<u>Committee members participating</u> (*indicates remote participant):

*Lisa Sotto, Chair
Jim Adler
*Suzanne Barber
J. Howard Beales III
*Craig Bennett
Allen Brandt
James Byrne
Renard Francois
*Melodi Gates
*Joanna L. Grama
*David Hoffman
Jeewon Kim
*Linda Koontz
*Joanne McNabb
Greg Nojeim
*Charles Palmer
*Julie Park
Christopher Pierson
*Tracy Pulito
Russell Schrader
*Barry Steinhardt
*Marjorie Weinberger
*Richard Wichmann

<u>Also in attendance:</u>

Jonathan R. Cantor, Acting DHS Chief Privacy Officer and Sponsor
Emily Andrew, Senior Privacy Officer, National Protection & Programs Directorate, DHS
Shannon Ballard, Designated Federal Official, Data Privacy and Integrity Advisory Committee
Tom Bush, Deputy Assistant Commissioner, Office of Intelligence, U.S. Customs and Border Protection, DHS
Laurence Castelli, Privacy Officer, U.S. Customs and Border Protection, DHS
Martha Landesberg, Senior Director, Oversight, Privacy Office, DHS
Christopher S. Lee, Privacy Officer, Science & Technology Directorate, DHS
Jeannette Manfra, Deputy Director, Enterprise Performance Management, Office of Cybersecurity and Communications, National Protection & Programs Directorate, DHS
J. Scott Mathews, Senior Advisor for Privacy & Intelligence, Privacy Office, DHS
Rebecca Richards, Acting Deputy Chief Privacy Officer and Senior Director of Compliance, Privacy Office, DHS
Steven Richards, DHS Privacy Office
Donna Roy, Executive Director, Information Sharing Environment Office, Office of the Chief Information Officer, DHS

Chair Lisa Sotto called the meeting to order at 2:10 pm.

DHS Acting Chief Privacy Officer's Update:

Mr. Cantor welcomed five new members to the Committee: Jim Adler, Allen Brandt, Julie Park, Russ Schrader, and Richard Wichmann. He noted the unplanned hiatus of the Committee due to a lack of a quorum as required by the DPIAC Charter and the impact sequestration is having on staffing, travel, and filling new vacancies. Mr. Cantor updated members on DHS Privacy Office (PRIV) activities that have occurred since the last meeting on November 7, 2012, including accomplishments of the Policy and Advocacy, Compliance, FOIA, and Oversight teams.

Policy and Advocacy

Mr. Cantor noted significant activities between the U.S. and Canada under the *Beyond the Border* initiative and PRIV's efforts to ensure implementation of the Joint Statement of Privacy Principles, particularly with the U.S. – Canada immigration information sharing agreement and the Entry-Exit program. There has been extensive engagement with the EU, including several negotiating sessions for the Data Privacy & Protection Agreement, the U.S. – EU Passenger Name Record Agreement review, the impact on EU relations after the Snowden/NSA incident, and the U.S. – UK visa and immigration information sharing agreement negotiated under the Five Country Conference. PRIV was a lead participant on the USG strategy on the review of 1980 OECD privacy guidelines, advocating for FOIA, E-GOV, and OMB guidance, which is reflected in the final document released on September 10.

To further raise awareness and promote DHS privacy best practices, PRIV presented at five training sessions organized by DHS headquarters for employees being deployed overseas titled "Understanding and Representing DHS Overseas." PRIV staff met with delegations from Norway, Japan, and the European Data Protection Supervisor to better inform international partners about the U.S. privacy framework, DHS compliance and FOIA programs, and DHS privacy policy and best practices.

Compliance

Mr. Cantor described how the Compliance team created and led a six-week boot camp and hosted its annual privacy compliance workshop, which registered 200 representatives from 45 agencies.

Mr. Cantor announced that the DHS FISMA score has improved steadily and is now at 89 percent for Privacy Impact Assessments (PIAs) and 98 percent for System of Records Notices (SORNs). In fact, between November 8, 2012, and September 1, 2013, the Privacy Office completed:

- 78 PIAs
- 20 SORNs
- 501 PTAs

Mr. Cantor noted that beginning on April 10, 2013, the DHS Privacy Office and Office of Civil Rights and Civil Liberties hosted a series of five bi-weekly briefings for privacy and civil liberties advocates on implementation of Executive Order (EO) 13636, "Improving Critical

Infrastructure Cybersecurity." These briefings allowed attendees to hear presentations by each of the working groups established by the DHS Integrated Task Force to implement the EO.

Mr. Cantor then discussed significant PIAs or SORNs published since the last DPIAC meeting including the Common Entity Index Prototype (CEI Prototype) SORN, the FIPPs based PIA on CBP's use of Unmanned Aircraft Systems (UAS), a PIA on Enhanced Cybersecurity Services, a PIA for CBP's Global Enrollment System, an updated and consolidated PIA for the Automated Biometric Identification System or IDENT, and three PIAs updating existing programs for sharing bulk information with the National Counterterrorism Center (NCTC).

Before getting into the subject matter on the agenda, Mr. Cantor noted that PRIV is involved in three work streams related to Unmanned Aircraft Systems: PIAs from DHS Science & Technology Directorate and Customs & Border Protection; the Privacy, Civil Rights and Civil Liberties UAS Working Group created to discuss DHS use of UAS and to make recommendations to the Secretary; and participation in interagency committees to consider numerous issues related to UAS, including privacy.

Freedom of Information Act

Mr. Cantor noted two FOIA related highlights since November 2012, including that in FY 2012, DHS received 190,589 FOIA requests – an increase of eight percent from FY 2011, and processed 205,895 requests – an increase of 41 percent from FY 2011. DHS also reduced its backlog by 33 percent in FY 2012 despite another record-breaking year in the volume of requests received.

DHS issued a policy memorandum in June 2013, titled "Updated Policy for DHS Application of FOIA Exemption 6 to DHS Personnel Information Contained within Agency Records", which provides updated guidance to ensure the Department processes personnel information contained within agency records in a consistent manner.

Oversight

Mr. Cantor discussed recent Privacy Compliance Reviews (PCRs) that covered a range of DHS programs, including:

- the use of social media for situational awareness in the National Operations Center's Publicly Available Media Monitoring and Situational Awareness Initiative;
- the E-Verify Self Check Program's use of a third-party identity proofing service.
- DHS' participation in the Nationwide Suspicious Activity Reporting Initiative;
- the Department's development of a classified, multi-agency, information sharing environment;
- the National Operations Center Counterterrorism Desk Database; and
- DHS implementation of the 2011 U.S.-EU Passenger Name Record (PNR) Agreement.

Mr. Cantor highlighted the review of implementation of the 2011 PNR Agreement, which included a review of DHS compliance with the terms of the international agreement as well as compliance with the PIA and SORN for the Automated Targeting System, the system in which PNR is stored. The findings for this review were published in July and Mr. Cantor led a joint

review with the European Commission, as was required under terms of the Agreement, on July 9 and 10.

Oversight continues to monitor implementation of recommendations flowing from two long-standing investigations that led to findings of non-compliance with DHS privacy policy specific to social media and information sharing. Mr. Cantor also noted PRIV response to a privacy incident involving a vulnerability in the software that a third-party vendor used to process personnel security investigations. Even though there was no evidence that any unauthorized user actually accessed any personally identifiable information, PRIV alerted potentially affected employees and contractors to the vulnerability, provided public notice on the DHS website, and managed a call center and email box to respond to inquiries.

Unmanned Aircraft Systems – Privacy & Departmental Use

Science & Technology (S&T) Directorate Privacy Officer, Christopher Lee, began his presentation with a discussion of terminology surrounding unmanned aircraft systems:

- UAVs – unmanned aerial vehicles: very small; do have cameras but cannot have weapons; FAA regulations prohibit civilian UAVs from being armed
- UAS – unmanned aircraft systems: a group of components working toward a common goal; communicates with ground, has sensors, and has pilot or auto pilot

S&T is currently surveying available UAS technology and uses with the goal of saving lives or property and to not impact privacy. Under the FAA Modernization and Reform Act of 2012, Congress directed the FAA to open national airspace to Small Unmanned Aircraft Systems (SUAS) (under 55 lbs). S&T's UAS PIA – the first PIA on the technology in the federal government[1] – outlines a project in partnership with the State of Oklahoma to test and evaluate SUAS for potential use by the first responder community and DHS operational components. S&T established a test program for SUAS in Fort Sill, OK and is posting the results online for federal, state, and local government agencies to use. This test site was chosen to limit privacy issues as 1) general members of the public do not have access to this base and 2) military bases are not under FAA control (so no FAA certificate of authorization is required). As the project proceeds, additional privacy measures were added, and with the results of this test phase, additional testing will move from Fort Sill, for example, to set up a search and rescue test in a national park or forest. Mr. Lee stressed that whatever the use of UAS, the operators will need to address all the FIPPs and that oversight and community outreach are equally important goals.

Customs and Border Protection (CBP) Privacy Officer, Laurence Castelli, gave an overview of the FIPPS analysis PIA for CBP use of UAS, including manned fixed-wing, unmanned fixed-wing, and manned rotary-wing aircraft. Mr. Castelli pointed out that CBP UAS are not armed, there is minimal personally identifiable information collected, and the information they do collect is for various missions, particularly for border operations. Mr. Casetlli highlighted certain FIPPs addressed in the PIA[2], including:

[1] November 2012: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_st_raps_nov2012.pdf

[2] September 2013: http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-aircraft-systems-20130926.pdf

- data retention (e.g., information that is collected on raw videos is maintained on DVR system for 30 days);
- purpose limitation (e.g., camera images include video and infrared images, radar looks for movement, and electronic signals are used for counterterrorism and/or smuggling interdiction); and
- security (e.g., encrypted feeds, limited access).

Scott Mathews, Senior Advisor for Privacy & Intelligence in the Privacy Office, differentiated between the term "drones" and UAS, explaining that drones have no pilots (they are programmed and fly around), while UAS have a pilot, but on the ground. Mr. Mathews complimented CBP noting that the FIPPs PIA is comprehensive and more detailed than people will expect and noted that, in addition to the S&T program, this is the only other UAS PIA from the federal government. Mr. Mathews gave greater insight into the Privacy and Civil Liberties UAS Working Group, explaining that they are exploring issues related to DHS use of UAS and that they have produced a "best practices" document based on the DHS FIPPs (in clearance as of September 12, 2013 and which will be publically available when finished). Additional topics still being considered by the Working Group include FEMA grants for UAS (where DHS is coordinating with the Department of Justice – which also has law enforcement grants, but the DHS FIPPs PIA would still apply); "loner drones" (if DHS supports state, local, tribal and territorial law enforcement partners, should there be a systematic process for how requests are submitted and fulfilled that can be audited?); and consideration of a broader review across the USG on all aspects of UAS (including discussion of FAA's efforts to expand commercial UAS).

A robust question and answer period from DPIAC members followed the UAS presentation, including questions on:

- collection of electronic signals/cell phone communication (DHS is monitoring open air signals, not encrypted or cellular traffic and above 18,000 feet; if communication is in border area, DHS has border authority with latitude in the law and may fall within border search exception; if not, depending on the type of investigation, DHS may secure a warrant or capture what is on open air waves);
- infrared signals or inadvertent data collection (DHS UAS do not have the ability to capture electronic signals; DHS UAS operating above 18,000 feet mostly in desert areas; electronic sensors not operating until over area of operations; border data collection basically dots moving around unless there is an encounter; image is not identifiable; important to note that if "dot" crosses an undefined area, law violation);
- DHS guidance for drones purchased with FEMA grant money (Working Group best practices still being drafted but could suggest FEMA put conditions on grand recipient, including creating a privacy policy and PIA; grant recipient UAS use for law enforcement and emergency search and rescue purposes); and
- definition of border (by regulation, CBP defines the border area as up to 25 miles into the interior; UAS Certificates of Authority can range from 25-60 miles from border; border patrol INA gives agents authority to stop someone to determine admissibility anywhere in the United States).

Although outside of the allotted public comment period for the September 12 meeting, the participating EPIC representative posed the following questions for which DHS responded on September 17:

- Q: Why was CBP PIA not written sooner? A: Based on the E-Government Act definition, CBP's UAS do not collect information in an identifiable form. Similarly, CBP's UAS do not collect information that can be retrieved by "some identifying particular" so any records collected by a UAS are not maintained in a system of records as defined by the Privacy Act of 1974. Therefore, neither PIA nor SORN is required under the law. However, under Section 222 of the Homeland Security Act of 2002, a PIA on the sensors deployed as part of the UAS was justified.
- Q: Explain why DHS presenter stated that UAS does not have signal interception capabilities, when CBP's March 2010 Performance Specification for UAS includes signal interception as a desired payload? A: Based on Section 3.2.1.2 of the March 2010 Performance Specification for UAS, DHS ultimately chose to acquire synthetic aperture radars (SAR) with ground moving target indicator mode (GMTI) and not signals interception receivers. CBP UAS do not have signals interception capability.
- Q: Does DHS use Spectral-matching technology? A: CBP does not use thermal infra-red sensors on its UAS and does not use spectral-matching technology.

Cybersecurity Executive Order – Integrated Task Force, Implementation and Privacy

National Protection & Programs Directorate (NPPD) Enterprise Performance Management Deputy Director, Jeannette Manfra, began her presentation with a discussion of the increasing risk of cyber attacks on our nation's critical infrastructure. Given that most of this infrastructure is owned by the private sector and not the U.S. government, she stated that it is vital that the DHS partnership with the private sector remain strong and that DHS supports American security and economic prosperity by strong cybersecurity initiatives. Ms. Manfra reviewed the Cybersecurity Executive Order (EO) and Presidential Policy Directive (PPD) deliverables and updated the DPIAC on its progress.

Ms. Manfra discussed establishment of the Integrated Task Force (ITF), which manages working groups to accomplish major deliverables and action items. These working groups are moving forward on an aggressive timetable to finalize deliverables; many of which are publically posted for review and comment.

NPPD Senior Privacy Officer, Emily Andrew, discussed the role of her office and described a five-step process to evaluate EO activities against the FIPPs. Ms. Andrew also identified programs affected by the EO and PPD and described her office's engagement with program managers.

Martha Landesberg, DHS Privacy Office Senior Director for Oversight, discussed the role of the Privacy Office (PRIV) and the Office of Civil Rights and Civil Liberties (CRCL) in implementing the EO. PRIV and CRCL attend all meetings and support all of the working groups as they encourage embedding privacy and CRCL assessments into the deliverables. The working groups have built a foundation for assessments that will be forthcoming in 2014. PRIV and CRCL co-chair the interagency working group on assessments. While the working group does not have a deliverable, it is composed of senior privacy and civil liberties officials of all

agencies implicated by EO and provides an effective forum to share each agency's activities. Lastly, PRIV and CRCL will compile an annual public report to President Obama on the privacy and CRCL impacts of EO activities, which is due in February 2014.

During the question and answer period, it was discussed that DHS needs to better communicate its plans and further explain long-existing programs, especially on protected critical infrastructure information (PCII), as part of the larger EO rollout. Ms. Andrew referenced the Protected Critical Infrastructure Information Management System (PCIIMS) PIA[3] that addresses the handling of PCII. Another question was raised as to how companies can volunteer their services either under or adjacent to the EO or if there was more flexibility in eligibility for the program. While some companies are aware of the programs and want to volunteer, they do not know if they are eligible or if they qualify as critical infrastructure. Ms. Manfra explained that while there is a legal definition as to who can participate, DHS is reaching out to stakeholders for participation and also looking at the full capabilities spectrum – from sophisticated cybersecurity practitioners to small businesses or others who are targets but have unsophisticated IT – and trying to tailor services to these different types of stakeholders.

Homeland Security Information Sharing Environment

Rebecca Richards, Acting Deputy Chief Privacy Officer and Senior Director of Compliance in the DHS Privacy Office, described how DHS has made a decision to change the way it handles DHS data. The Privacy Office is working closely with this program to ensure that privacy is built into this program and the panelists discussed the overall DHS data framework and two pilots and prototype that are being launched.

Ms. Richards thanked the Committee for their December 2011 recommendations[4] and noted that this guidance continues to inform the department's discussions and decisions in this area. She noted that the department's knowledge and understanding of how DHS handles its data and the environment in which we work (both from a mission perspective and a technical perspective) has changed and therefore our approach to the use and sharing of DHS data has changed. These changes include system limitations (such as an across the board federated query system), the need to "see" across DHS; and interactions with the intelligence community. However, the department is actively incorporating DPIAC recommendations on access and use controls; applicable privacy policies (including completing PIAs – four pending – and SORNs throughout the pilot process); data integrity; audit trails; data security and retention; and redress.

Tom Bush, Deputy Assistant Commissioner, Office of Intelligence, U.S. Customs and Border Protection, discussed the mission problems this information sharing environment aims to alleviate. He noted that there are stove piped systems, multiple log-ins, and that different systems deliver different search results; all contributing to inefficient use and sharing of homeland security information, which is an operational impact.

Mr. Bush chairs the Common Vetting Task Force (CVTF), which is made up of DHS components including PRIV and CRCL, and which was created to move programs forward as

[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_pciims_foc.pdf
[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report_2011_01.pdf

"ONE DHS". The CVTF continues to discuss these mission needs and to move forward on solutions together. DHS pilot programs began with access to 2-3 data sets in a way that tests the access controls but allows DHS to do analysis if an operator has additional access rights. These pilots are testing these capabilities and will not move into an operational state until there is a demonstrated ability to control and safeguard DHS information while supporting operational needs.

Donna Roy, Executive Director, Information Sharing Environment Office, Office of the Chief Information Officer, discussed recent progress in controlling access and use of the data via access control authorization policies. By employing access safeguards, operators can still get to the data quickly, interpret it better, and get more consistent results. Some access controls being testing include person attributes, context/use, and data tags, although these access controls remain dynamic to ensure appropriate access and appropriate use.

The panelists discussed three major pilot activities that are currently underway:

- Neptune – data is not accessible to an officer or employee, but data is tagged and ingested in a "big data" platform on the SBU platform then shared with CEI Prototype and Cerberus Pilot (but not accessible for other purposes).
- CEI Prototype – also on the SBU platform, this pilot receives a subset of the tagged data from Neptune and correlates data across component data sets. Tests the way to collect a minimal amount of biographic data in a meaningful way.
- Cerberus – resides in the TS/SCI domain and receives tagged data from Neptune to test the ability to ensure that only users with certain attributes are able to access data that is based on define purposes.

Questions from members followed the panelists' prepared remarks, including comments on tagging data elements; avoiding inappropriate access (i.e., insider threat) through robust and automated audit logs; data retention (particularly if different source systems have different retention period): data integrity (particularly with non-Roman character names); false positive metrics; automatically populating changes from source data; pattern based queries with appropriate purpose/use contexts; use limitation from data users (considering use, context, purpose, and access rights for that user); confirming there is no central database that contains the results of all queries; and audit logs to store who queried and what they queried but not the results of the query.

Policy Subcommittee Draft Recommendations/Committee Discussion

Joanne McNabb, Chair of the Policy Subcommittee, presented to the Committee a draft report that included recommendations to the Department on the use of live data for research, testing or training. A copy of the draft report was posted on the DPIAC website in advance of the meeting to allow for public review. Ms. McNabb summarized the subcommittee's research, which included briefings from DHS privacy officers from CIS, ICE and S&T that each discussed programs that use live data. The subcommittee considered the benefits and potential risks of using live data, and then proposed a process for components to authorize the use of live data, including the creation of an intake questionnaire and recommended controls on the department's use.

Committee Discussion

The Committee discussed additional language regarding contractual obligations, the need to provide the legal basis for the use of the data, and clarified references to health data. Minor edits were made to the subcommittee's draft report then a motion was made to approve the updated draft as a full Committee report. There were no dissenting votes, so the report was made final with the agreed upon edits.

Public Comments and Close of Meeting

Chairman Sotto then provided an opportunity for members of the audience to address the Committee. As there were no further public comments, Chairman Sotto adjourned the meeting at 6:00 pm.

The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of DHS and the Chief Privacy Officer of DHS on programmatic, policy, operational, administrative, and technological issues within DSH that relate to personally identifiable information (PII), as well as data integrity and other privacy-related matters. Materials presented to the Committee, including all Committee reports and recommendations, meeting summaries, and transcripts where available, are posted on the Committee's web page on the DHS Privacy Office website, www.dhs.gov/privacy.

Attendance

DPIAC Members
Jim Adler
Suzanne Barber
J. Howard Beales III
Craig Bennett
Allen Brandt
James Byrne
Renard Francois
Melodi Gates
Joanna L. Grama
David Hoffman
Jeewon Kim
Linda Koontz
Joanne McNabb
Greg Nojeim
Charles Palmer
Julie Park
Christopher Pierson
Tracy Pulito
Russell Schrader
Lisa Sotto
Barry Steinhardt
Marjorie Weinberger
Richard Wichmann
Jonathan R. Cantor
Dianna Carr
Laurence Castelli
Bob Davis
Cindy Falkenstein
Vicki Fresenko
Mark Freeman
Elizabeth Geffin
Martha Landesberg
Christopher S. Lee
Lindsay Lennon
Liz Lyons
Jeannette Manfra
J. Scott Mathews
Peter Pietra
Rebecca Richards
Steven Richards
Donna Roy
Akbar Siddiqui
Dayo Simms

DHS
Emily Andrew
Shannon Ballard
Catherine Bauer
Tom Bush

Public
Tim Barnes, MITRE
David Husband, EPIC
Lauren McCollum, Lockheed Martin
Jeramie Scott, EPIC
Dale Smith, Lockheed Martin
Joe Silver, ACLU
Megumi Yukie, EFF