Data Privacy and Integrity Advisory Committee
Public Meeting
September 22, 2014

Committee Members Participating (*indicates remote participant):

Lisa Sotto, Chair
Jim Adler
Sharon Anolik
Craig Bennett
Allen Brandt
Alan Broder
James Byrne
Josh Galper
Melodi Gates
Lynn Goldstein
Joanna L. Grama
Jeewon Kim*
Linda Koontz
Debbie Matties
Joanne McNabb
Sarah Morrow
Greg Nojeim
Charles Palmer*
Julie Park
Christopher Pierson
Tracy Pulito
Russell Schrader
Barry Steinhardt*
C. M. Vandervoort
Marjorie Weinberger
Richard Wichmann

DHS Presenters:

Shannon Ballard, Designated Federal Official, Data Privacy and Integrity Advisory Committee
Karen Neuman, Chief Privacy Officer, U.S. Department of Homeland Security (DHS)
Andy Ozment, Assistant Secretary for Cybersecurity & Communications, National Protection and Programs Directorate, DHS
Kellie Cosgrove Riley, Senior Director for Privacy Policy & Advocacy, Privacy Office, DHS
Donna Roy, Executive Director, Information Sharing Environment Office, Office of the Chief Information Officer, DHS
Clark Smith, Director, Knowledge Management Division and Chief Information Officer, Office of Intelligence & Analysis, DHS

Opening Statement

Shannon Ballard, Designated Federal Official for the Data Privacy and Integrity Advisory Committee (DPIAC), formally opened the meeting. The DPIAC meeting was hosted in person and via a live video feed to increase participation from DPIAC members and the public. DPIAC Chair Lisa Sotto called the meeting to order at 2:00 pm.

DHS Privacy Office Update

Karen Neuman, DHS Chief Privacy Officer, delivered remarks on activities of the DHS Privacy Office since the DPIAC's last public meeting in January 2014. Neuman welcomed the newly appointed members to the Committee (Anolik, Broder, Galper, Goldstein, Matties, Morrow and Vandervoort), announced that a Federal Register Notice was published (September 22) soliciting new applications for DPIAC membership, and noted that the Privacy Office Annual Report

would be published in short order[1]. Neuman reviewed changes to Privacy Office staffing as well as revisions to the Privacy Office Strategic Plan to determine how office goals and objectives should be adjusted to reflect the current environment and to link to the Quadrennial Homeland Security Review and the Secretary's priorities.

Outreach

Neuman discussed Privacy Office outreach to relevant stakeholders, including Congressional Subcommittees and the privacy advocacy community, to discuss Unmanned Aircraft Systems, the DHS Data Framework, and to provide greater transparency into office activities.

International

In connection with the *U.S. – Canada Beyond the Border (BTB) Action Plan*, Neuman updated the Committee on implementation of the Plan, including development of flexible training materials on the BTB Privacy Principles, review of all BTB information sharing agreements, and implementation of Phase III of the BTB Entry/Exit Program. The Privacy Office continues to participate in negotiations with the European Union (EU) for a U.S. – EU umbrella agreement that would provide a framework for facilitating the exchange of law enforcement information. One key discussion point is how the U.S. could satisfy the EU's requirement that EU citizens enjoy the right of judicial redress for wrongful disclosure or refusal to correct inaccurate information equally as U.S. Persons enjoy under the *Privacy Act of 1974*. Separately, the Five Country Conference created a new Privacy Task Force to assess the privacy and information sharing laws and policies of the member countries and how they may impact information sharing goals. Privacy Office staff act as the lead for the Department on the Privacy Task Force, and were successful in obtaining agreement among all five countries to proactively share with one another their full Privacy Impact Assessments (PIAs) for all Five Country Conference projects.

National Security

Privacy Office Senior Advisor for Information Sharing, Ken Hunt, began a detail in May 2014 at the National Counterterrorism Center (NCTC) as DHS's first on-site oversight representative. He will review NCTC's compliance with its information sharing agreements with DHS and will work on an overarching PIA to provide more transparency regarding DHS's information sharing relationship with NCTC. The Privacy Office also discussed with the Office of the Director of National Intelligence (ODNI) and interagency partners the privacy implications of sharing non-Title 50 information with the Intelligence Community and continues to participate in the DHS Records Working Group to review sensitive national security information sharing activities and policies.

Information Sharing Governance

The Privacy Office maintains an active leadership role in DHS's internal information-sharing and management governance processes. Through participation in the DHS Information-Sharing and Safeguarding Governance Board, the Privacy Office helped develop the DHS Information-Sharing and Safeguarding Strategy and its implementation plan, which includes a priority objective for privacy, civil rights, and civil liberties compliance processes. Through participation in the DHS Information-Sharing Coordinating Council's Data Access Request

[1] Published 10/1/14 http://www.dhs.gov/publication/dhs-privacy-office-2014-annual-report-congress

Process Working Group, the Privacy Office helped memorialize and automate DHS's internal clearance processes for domestic information-sharing agreements and ensured that the oversight bodies (including the Office of General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties), are able to review DHS agreements with external entities.

Training

The Privacy Office continues to use training to "bake" privacy into the activities of the Department. One specialized training that was recently held was for the DHS Office of the Chief Human Capital Officer where Privacy Office staff trained all Headquarters staff on best practices for safeguarding personally identifiable information (PII). So far this fiscal year, the office has trained over 125 DHS officers that will be posted overseas via the international privacy policy module to raise awareness about U.S. privacy law and DHS privacy policy and practice. In June 2014, 196 personnel from 42 federal agencies attended the DHS annual privacy workshop, which provides in-depth training on all of DHS privacy compliance processes and best practices and other important privacy topics.

Compliance

Neuman highlighted high profile compliance undertakings (out of the 33 PIAs and 11 SORNs published since January), including those to implement the DHS Data Framework and CBP's Border Surveillance Systems. The Privacy Office played an extensive role in the development of the Unmanned Aircraft Systems (UAS) Privacy Civil Rights and Civil Liberties Working Group's draft best practices document for using UAS. The Working Group is also developing guidance that might be appropriate for state and local grant recipients who intend to use some or all of DHS funds received to purchase UAS.

FOIA

As the DHS Chief Freedom of Information Act Officer, Neuman noted that this year alone DHS has proactively posted 3.8 million pages of records, eclipsing the combined total of the previous five years.

Oversight

Privacy Compliance Reviews (PCRs) are designed to assess highly privacy-sensitive programs' compliance with existing PIAs and SORNs. In August, the EINSTEIN PCR was completed with favorable results and the PCR on the Enhanced Cybersecurity Services Program is underway (which was noted in the DHS assessment of the Cybersecurity Executive Order).

DHS Cybersecurity Overview

Andy Ozment, Assistant Secretary for Cybersecurity & Communications (CS&C), National Protection and Programs Directorate (NPPD), provided an overview of DHS cybersecurity activities. Ozment explained that NPPD looks to protect critical infrastructure from all hazardous threats and within NPPD, C&SC focuses particularly on cybersecurity and communications and making it resilient. CS&C does this by helping its customers manage risk and be resilient in an environment where the interconnectedness of infrastructure and cyberspace are increasingly resulting in "fragility" of that critical infrastructure. CS&C helps its customers understand and manage their risks; reduce the frequency and impact of any incidents that occur; and build capacity, all while protecting the privacy and civil liberties of the customer.

Ozment discussed implementation of Executive Order 13-636 through information sharing, raising cybersecurity best practices across critical infrastructure, and incorporating privacy and civil liberties best practices through the cybersecurity framework (noting a National Institute of Standards and Technology led effort on developing privacy best practices). Information sharing means sharing quality and timely cyber threat information with the private sector (through the DHS National Cybersecurity and Communications Integration Center), while incorporating privacy best practices to retain trust in the relationship.

Ozment discussed specific cyber programs, including the EINSTEIN program, which is for the federal government only providing "perimeter defense" (i.e., checking what is coming in and out). EINSTEIN monitors network traffic (not people) and acts upon known indicators of malicious activity. Enhanced Cybersecurity Services (ECS) is similar to the EINSTEIN system, but is only focused on the private sector, where DHS takes classified threat information and appropriately passes that information to private sector service providers. DHS responders to cyber intrusions receive privacy training and typically do not access the private company's data, but guide them in their cyber response.

Ozment then took questions from the DPIAC Members. Chair Sotto asked if there was guidance from DHS on what information companies should not share with the government or guidance on how to protect PII when it does need to be shared. Ozment noted that CS&C's goal is help the impacted organization get back up and running as well as to help the organization understand the extent of the intrusion or attack. From this, DHS takes the lessons learned and shares that information with other private sector companies so they can avoid the same intrusion or attack. DHS staff who work on these cases have robust privacy training and standard operating procedures so the organization retains oversight and responsibility for any PII involved.

Member Pierson asked about State and Local organizations that have taken advantage of Multi-State Information-Sharing Analysis Center (MSISAC) services. MSISAC operates as the equivalent of the private sector information-sharing and analysis centers that are helping individual sectors be cognizant of and mitigate cyber threats (funded each year in part by a grant from DHS.)

Additionally, Member Nojeim questioned the timeliness and usefulness of the DHS cyber alerts to the private sector. Ozment agreed there is work to be done to improve the speed with which information is shared, but he countered that over the last five years the private sector's knowledge of what is happening with respect to cyber threats has increased dramatically and the government's cyber threat information is less unique than it once was when there was a less robust private sector market surrounding this space.

Member Adler asked if DHS is tracking when it incorrectly identifies a URL as malicious and what is done with that information. Ozment noted that DHS is working closely with the private sector and improving incentives to ensure the information provided by DHS is accurate, timely and unique.

DHS Data Framework

History and Pilot Success

Clark Smith, Director, Knowledge Management Division and Chief Information Officer, Office of Intelligence & Analysis, led off the DHS Data Framework panel by discussing where DHS fits in with the intelligence community and the Data Framework pilot projects leading to a limited implementation plan. Smith described the need to take DHS data (unclassified, operational, or DHS Homeland Security data) and noted the challenge when searching DHS unclassified data with classified criteria or classified information. To do a search like this, the first step would be to search DHS data with classified indicators or classified information and conduct the search in a way that protects the sources and methods of the classified data, yet at the same time make the connections to protect the homeland. DHS recognized the limitations in this process and launched its "big data" pilots, fully considering the privacy, civil rights, and civil liberties implications of such a system and building capabilities to protect the data while meeting the mission (such as governance and oversight, immutable auditing and logging, access controls, etc.).

The pilots started with three data sets (Alien Flight Student Program, Student and Exchange Visitor Information System, and Electronic System for Travel Authorization) from three DHS components (CBP, TSA, and ICE). In the pilot, each data set is "wrapped" with its use authorities, why and how it was collected, and who can do what with the data. The Neptune system was then built to collect the "wrapped" data on the unclassified side. With the policy "wrappers" in place, the data is properly tagged and appropriate oversight is built in. On the classified side, classified search parameters are conducted in the Cerberus system and on the unclassified side, the search is done via Common Entity Indexing. Not only were the pilots successful from a searching perspective, but from an oversight perspective, all user movements, user requests, query strings, permissions, and results were effectively tracked to ensure compliance.

Lessons Learned

Kellie Riley, Privacy Office Senior Director for Privacy Policy & Advocacy, discussed the lessons learned from the pilots, which included:

1. Governance – establishing a strong governance process that includes privacy and civil rights and civil liberties in order to evaluate the integration of new data sets as the Data Framework develops new missions, new uses, and new analytical tools.
2. Incremental Development – it is important, in a complex system, to take a small portion first to best determine the rules before expanding.
3. Redress and Refresh – as the Data Framework matures, need the ability to refresh the data in a timely manner, and ensure corrections are made as appropriate.
4. Stakeholder Engagement – important that the mission users and operators understand the value of the Data Framework and are willing to use it.
5. Transparency – in addition to privacy compliance documents, continue to engage privacy and user communities.

Limited Production Capability

Donna Roy, Executive Director of the Information Sharing Environment Office in the DHS Office of the Chief Information Officer, discussed plans to implement the lessons learned and move the pilots into limited production. Limited production means using the same data sets from the pilots with limited users, but using all of the data for each of those data sets for as long as the current retention period allows for real analytical use. The goal for limited production capability is to not only understand how the users are going to apply their analytical processes and use the tools provided to solve real problems, but to also continue "mission case development", which reviews each user and use of the data provided. Another goal is to get to near real-time on some of the data sets and to continue to refine the oversight mechanism. Limited production capability will lead to a draft of a concept of operations (CONOP) document to also determine how to best handle data quality and data redress issues.

The panelists took questions, where Member Pierson asked about the success criteria (key performance indicators or KPI) for increasing the number of users and agencies that have access to the Framework or increasing the databases outside of the current three that were rolled into the underlying pilots. Smith replied that generally the main success criteria is data, in that the available data ties back to what is needed in the use cases and the analyst has access to the right data needs to ask the questions in response to the threat. A KPI regarding users would be if the right analyst had the right access to the right information at the right time. As for agencies, Smith believes the DHS components with access are appropriate for now, but if it came to be that another component or non-DHS agency requested access, their authority to collect the data and DHS' authority to disclose the data would have to be carefully considered. Riley opined that an important KPI is related to the safe use of the data, given the access controls and the capability for oversight offices to understand the audit logs and measurable controls for abnormal behavior using those logs.

Member McNabb asked about "scaling the program up" and moving toward increased automation when tagging the data. Riley responded that once the Framework gets to the tipping point (approximately eight or nine data sources), data tagging becomes an "80-20 rule" of known tags and exceptions. The real driver, however, is how quickly the targeted sources can get to near real-time capabilities, so that the Framework provides the freshest data possible for the analytical efforts.

Member Steinhart asked about effective redress or error correction when the data subjects can't know that they are under consideration and how/if redress can be built into the Data Framework under those circumstances. Riley confirmed that there are some use systems that have exemptions under the Privacy Act that will not allow for access or amendment of information. However, if a redress request is made that DHS complies with, the intent is for any correction to lead back to the source data (regardless of exemption) so future users of that data will have the most correct information possible. Those amendments may not go back to the individual user or the person who submitted the data, but it will actually go back to improving the quality of the data so that better decisions are made with hopefully better outcomes.

Subcommittee Drafts on DHS Data Framework Tasking - Transparency & Oversight

Policy Subcommittee – Notice and Transparency

Joanne McNabb, Chair of the DPIAC Policy Subcommittee, summarized the subcommittee's research efforts and its findings that would impact the pilots plus any future iteration of the Data Framework. Succinctly, the subcommittee believes DHS should develop other ways to disclose more specific information on other future potential users and uses than what can be disclosed at the time of collection of the distinct sets. The three recommendations in the draft report included 1) improving existing notices to ensure effective communications for the intended audiences; 2) supplementing printed Privacy Act notices with "living" internet-based information that can be more specifically updated as new uses and new users are involved; and 3) conducting specific outreach activities with impacted data subjects to provide a greater understanding of the way that DHS uses their information. The full committee fine-tuned the draft recommendations, and then voted to accept the updated draft as a final DPIAC recommendations document.

Technology Subcommittee – Audit & Oversight

Joanna Grama, Chair of the DPIAC Technology Subcommittee, discussed the subcommittee's research efforts to develop recommendations about audit processes, access controls, and oversight. The key aspects of the audit recommendations were to ensure that the audit logs contain enough information or indicators to address system operational performance and efficacy, as well as enough information to investigate potential use anomalies. The key aspects of the access controls and oversight recommendations were to ensure that access controls are in place to restrict access to the systems and information only to users with legitimate needs to use that data and who have received appropriate training, and that any changes to access control systems are recorded and reviewed for appropriateness. The full committee fine-tuned the draft recommendations, and then voted to accept the updated draft as a final DPIAC recommendations document.

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 4:50 pm.

Drafted by Shannon Ballard, DPIAC Designated Federal Official, October 24, 2014

Certified by Lisa Sotto, Chair, DPIAC, October 27, 2014

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, http://www.dhs.gov/privacy-office-dhs-data-privacy-and-integrity-advisory-committee.

Appendix

Additional Participants (* denotes remote participant)

Emily, Andrew, DHS NPPD
Hafiva Arikat*, Homeland Security Intergovernmental Affairs
Diane Bjornson*, DHS FEMA
Jonathan Cantor, DHS PRIV
Dianna Carr, DHS NPPD
Katheleen Claffie, DHS PRIV
John Conors, DHS CBP
John Curran*, Telecommunications Reports
Debra Danisek, DHS PRIV
Jamie Danker*, DHS Citizenship and Immigration Services
Andrew L. Ehrlich*, Faegre Baker Daniels LLP
Kathryn Fong*, DHS FEMA
Victoria Fresenko, DHS CMO
Michael Frias*, DHS
Jordan Gottfried, DHS PRIV
Karyn Higa-Smith, DHS S&T
Leslie Jensen*, DHS
Tony Johnson, DHS TSA
Ashley Kirkland, DHS NPPD
Scherida Lambert, DHS NPPD
Christopher Lee*, DHS S&T
Lindsay Lennon, DHS PRIV
David Lindnes, DHS NPPD
Vania Lockett, DHS NPPD
Drew Mitnick, Access Now
Jameson Morgan, DHS PRIV
Karen Neuman, DHS PRIV
Andy Ozment, DHS NPPD
Grace Pardo*, Deloitte
Peter Pietra, DHS TSA
Lane Raffrey*, DHS FEMA
Kellie Riley, DHS PRIV
Donna Roy, DHS CIO
Lauren Saadat, DHS PRIV
Art Sepeta, DHS I&A
Dayo Simms, DHS S&T
Allison Tanaka*, U.S. Secret Service