

DEPARTMENT OF HOMELAND SECURITY
MEETING OF THE
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

Thursday, September 10, 2015

650 Massachusetts Avenue, N.W.
4th Floor
Washington, D.C.

The meeting was convened, pursuant to
notice, at 1:05 p.m., LISA J. SOTTO, Chair,
presiding.

ATTENDANCE

COMMITTEE MEMBERS PRESENT:

Lisa J. Sotto, Chair

Jim Adler

Sharon A. Anolik

Allen Brandt

James M. Byrne

Joshua Galper

Joanna L. Grama

Joanne McNabb

Christopher Pierson

Barry Steinhardt

C.M. Toke Vandervoort

Marjorie S. Weinberger

Richard Wichmann

ALSO PRESENT:

Dan Chenok, Chair, Cyber Subcommittee, Data Privacy
and Integrity Advisory Committee

John Connors, Privacy Officer U.S. Customs and
Border Protection, DHS

Kellie Cosgrove Riley, Senior Director, Privacy

Policy and Oversight, DHS

Jamie Danker, Director, Senior Privacy Officer
National Protection and Programs Directorate,
DHS

Christopher Drew, Project Manager, Public Cloud,
ESDO, DHS

Jeffrey Eisensmith, Chief Information Security
Officer, DHS

Douglas Hansen, Director (Acting), Cloud Enterprise
Services, ESDO, DHS

David Lindner, Privacy Analyst, DHS

Karen L. Neuman, DHS Chief Privacy Officer

Rob Palmer, Deputy Executive Director (Acting),
Enterprise System Development Office (ESDO),
DHS

Sandra L. Taylor, Director of Administration,
DHS Privacy Office

P R O C E E D I N G S

MS. TAYLOR: Welcome, everyone. I am Sandra Taylor. I am the designated Federal official for the Data Privacy and Integrity Advisory Committee. On behalf of our members, welcome to our first and only meeting in fiscal year 2015.

I am just going to go over some housekeeping items for you. The restrooms are out the door to the right. We ask that you silence your phones, please. If you have any questions on the slides, if you do not have copies of the slides, please see me, and I will make sure copies are provided to you.

At this time, I want to take a roll call of our members on the phone, okay?

Jim Adler?

MR. ADLER: I'm here.

MS. TAYLOR: Sharon Anolik?

MS. ANOLIK: Here.

MS. TAYLOR: K. Suzanne Barber?

[No response.]

MS. TAYLOR: Allen Brandt?

MR. BRANDT: I'm here.

MS. TAYLOR: Alan Broder?

[No response.]

MS. TAYLOR: James Byrne?

MR. BYRNE: Here.

MS. TAYLOR: Josh Galper?

MR. GALPER: Here.

MS. TAYLOR: Melodi Gates?

[No response.]

MS. TAYLOR: Lynn Goldstein?

[No response.]

MS. TAYLOR: Joanna Grama?

MS. GRAMA: I'm here.

MS. TAYLOR: Jaewon Kim?

[No response.]

MS. TAYLOR: Joanne McNabb?

MS. McNABB: Here.

MS. TAYLOR: Sarah Morrow?

[No response.]

MS. TAYLOR: Charles Palmer?

[No response.]

MS. TAYLOR: Christopher Pierson?

MR. PIERSON: Here.

MS. TAYLOR: Tracy Pulito?

MS. PULITO: I'm here.

MS. TAYLOR: Russ Schrader?

MR. SCHRADER: Here.

MS. TAYLOR: Lisa Sotto?

MS. SOTTO: Here.

MS. TAYLOR: Barry Steinhardt?

MR. STEINHARDT: Here.

MS. TAYLOR: Toke Vandervoort?

MS. VANDERVOORT: Here.

MS. TAYLOR: Marjorie Weinberger?

MS. WEINBERGER: Here.

MS. TAYLOR: Richard Wichmann?

MR. WICHMANN: Here.

MS. TAYLOR: Okay. With this roll, it establishes a quorum. At this time, I am going to turn the meeting over to Lisa Sotto, who is our chairwoman.

MS. SOTTO: Thank you so much, Sandy.

I am delighted to welcome our committee members, our speakers, and members of the public who

have joined us.

I would ask you to please silence your cell phones.

For those of you who are listening by phone, please do speak up, if you're having trouble hearing any of us. You should just be aware that the slides will be a little bit delayed, so as we turn to a new slide, there may be a second or 2 delay.

We have an operator-assisted call, so if you need assistance on the phone, please do be aware that there is somebody there to assist you.

We are going to take questions from members from the public at the end of the meeting, so if anybody wants to ask a question, there is a registration sheet outside the room. Please go ahead and sign up, and we will take about 15 minutes of questions from any member of the public who would like to speak.

We have a full agenda. We are going to be talking about privacy incidents, mobile applications, and then we will hear an update from

our Cybersecurity Subcommittee on our algorithmic analytics initiative report.

Let's see, just one note about the public comment period. We may start a little bit early, if the prepared sessions run short. So if you are a member of the public, either on the phone or in the room, we may start a bit early.

If you are the phone and a member of the public, you obviously can't sign up, but we will take questions first from those who are here live present, and then we will take questions from those of you on the phone.

I am delighted to welcome Karen Neuman, the chief privacy officer of DHS. Karen was appointed in October 2013, and in her role as chief privacy officer, she is responsible for evaluating department-wide programs, systems, technologies, and rulemakings for potential privacy impacts, and mitigating those impacts. And together with her office, she is responsible for privacy compliance across DHS. Karen also serves as the department's chief Freedom of Information Act officer.

We are eager to hear about your activities and the activities of your office. Please proceed.

MS. NEUMAN: Thank you, Lisa.

Good afternoon. I want to thank all of you for taking time to attend this meeting in person and on the phone. And I particularly wanted to thank all the DPIAC members, the experts, the subcommittee experts, and members for the incredible commitment and time they spend providing guidance to us through the Data Privacy and Integrity Advisory Committee.

As Lisa indicated, we have a very full agenda, and I am going to kick it off by giving you an overview of some of our activities over the past fiscal year.

We do have our annual report that is going to be published soon, which will provide a lot of information about what we have been doing, and I would encourage all of you to come and take a look at it. Here are a few key highlights.

Last year, I announced that we were in the process of updating the Privacy Office strategic

plan. In December 2014, we finalized the plan for fiscal years 2015 through 2018. The plan included a minor reorganization of the Privacy Office, which is an important initiative that I think aligns the work of the office with new issues, evolving priorities, and a new fiscal environment that is, frankly, here to stay for the foreseeable future.

The revised plan does reflect some changes to our privacy teams and articulates our missions, goals, and values for the office.

You may recall that, in the past, our privacy teams consisted of privacy oversight, privacy compliance, privacy policy. In light of the growth of information-sharing within the department, we have combined the oversight and policy teams, and we also created a new security safeguard and information-sharing team function.

Kellie Cosgrove Riley, who many of you may know, serves as the senior director of policy and oversight. Debra Danisek serves as our senior director for compliance. And Ken Hunt serves as the senior director for the newly created information-

sharing, security and safeguarding team.

As you know, the DHS Privacy Office has some of the best, if not the best, privacy professionals in the profession. Because of that, some of them have moved on, but it also creates room to hire new staff, and I wanted to share with you some of those developments.

James Holzer, who many of you may know, was our former senior director of FOIA operations. He left in August to take on the role of the head of the Office of Government and Information Services, which is an office inside the National Archives and Records Administration. There he is overseeing agency compliance with the Freedom of Information Act and government-wide FOIA policies.

We are in the process of filling the position, and we hope to fill it very soon, although we are quite confident that we will never be able to fill James' shoes. Those of you who had the opportunity and good fortune to work with him will know exactly what I mean.

In August, two new employees joined the

Privacy Office. David Dolph joined the compliance team as a privacy analyst. Previously, he worked for DHS handling FOIA requests for USCIS in Lee's Summit, Missouri.

Heela Hamidi joined the office as our executive secretary and director of correspondence.

Prior to joining the Privacy Office, she worked in the main Office for the Executive Secretary at DHS.

In July, Gina Mostafaie joined the compliance team. She came from ICE and previously worked as a behavioral detection officer at TSA.

In March, David Lindner joined the privacy policy and oversight team. He previously worked as a privacy analyst at NPPD in their Privacy Office. Some of you may know him from his former tenure there. He is going to be presenting here as well, and we are very happy and delighted to have David on the team.

And then, as many of you may know, Naomi Parnes joined the Privacy Office as my special assistant. Prior to joining DHS, Naomi worked on telecommunications and privacy at the Federal

Communications Commission and at the Federal Trade Commission.

We also welcomed two detailees from CBP privacy, Larry Castelli and Marilyn Powell.

As you know, this office does a tremendous amount of outreach to the privacy advocacy community and to others who are interested in the work that we do. We have continued assiduously in those efforts.

We are very committed to maintaining a dialogue with the advocacy community.

In that vein, I continue to host targeted meetings with the privacy advocates on areas that I believe will be of interest to them.

This year, the Privacy Office organized four briefings for the privacy advocates. Starting in October, Dr. Andy Ozment, who was then Assistant Secretary of the Office of Cybersecurity and Communications within NPPD, discussed cyber programs at DHS, including the EINSTEIN program, enhanced cybersecurity services, general information-sharing, and incident response.

In November, we briefed the privacy

advocates on an initial PIA, a Privacy Impact Assessment, regarding the use of license plate readers at ICE through a solicitation that ICE procured.

In January, we held a briefing at NPPD on proposed cyber legislation.

Finally, in June, we hosted a briefing by NPPD on the DHS automated indicator-sharing program.

As you may know, I also had the pleasure of testifying before the House Committee on Oversight and Government Reform in June on FOIA operations and transparency here at DHS. Then last week, my deputy chief FOIA officer, Dolores Barber, and I followed up with an informal staff briefing on some outstanding questions that they had.

We hope to continue our discussions with our oversight committees on FOIA policy and operations within the department, including our backlog and our backlog-reduction efforts, which I am very happy to say are trending in the right direction. We have reduced the backlog significantly and are looking forward to continuing

to do so due to the efforts and initiatives that have been put in place by Dolores and James, when he was here. I will talk about that a little bit later.

I have also been active and the office has been very active in supporting me in the international arena. As you may know, we recently concluded the Privacy Office review of the U.S.-EU Passenger Name Record Agreement. In February 2015, the Privacy Office initiated its review in conjunction with a privacy compliance review of adherence to the terms of the agreement and compliance with the PIAs for relevant systems.

Over several months, the Privacy Office, specifically Shannon Ballard, who many of you may recall from her work with this committee, analyzed existing policies and procedures relevant to the PNR agreement, reviewed other documentation, and received briefings and conducted site visits, and interviewed key managers, officers, and analysts who handle PNR within DHS.

Shannon completed her review by publishing

a final report on June 26 that found DHS's PNR policies and practices, including how PNR is received, used, and disseminated by CBP, to be substantially compliant with the 2011 agreement and related provisions in the appropriate Privacy Impact Assessments and System of Record Notice.

That said, the Privacy Office made 12 recommendations to improve privacy protections and increase compliance with the terms of the agreement. Key recommendations focused on improved transparency, use limitation, and accountability.

Following the PCR, the privacy compliance review, we hosted a five-member delegation from the European Commission on July 1 to 2 to conduct the actual joint review of the PNR agreement. The EU delegation consisted of representatives from the EC's Home Affairs and Justice Directorates, the French Data Protection Authority, and a representative from the U.K. Home Office.

In preparation for the review, we also responded to 84 prepared questions from the commission. We worked closely with CBP and some of

our other components to address those questions.

The PCR, as it has in the past, as have the questions, formed the basis for the review. They were very helpful in terms of teeing up the department to anticipate any wrinkles or any issues that might have come up during the review, and really formed the basis for the review and kind of framed the approach.

The EU delegation was briefed at the National Targeting Center and shown system functionalities to limit user access, mask sensitive terms, secure data, and conduct audits, as well as provided additional information on CBP targeting methodologies. These demonstrations, in terms of the functionalities they were shown, really were aligned with the privacy protections that are embodied in the agreement.

We also arranged for additional briefings to address redress, oversight, and other DHS components' use of PNR for authorized purposes.

This is kind of a sensitive time in the EU. There is a lot of activity, as you know, on the

privacy front. But we do expect the commission to write a largely favorable report, if their comments during the joint review itself are any indication. We expect the report to be published sometime this fall.

On other international engagements, you may have read the press release from the Department of Justice that the U.S.-EU Data Protection and Privacy Agreement, the DPPA, which has been slogging around for a number of years, was finally finalized earlier this week. On Tuesday, September 8, it was initialed by representatives from the EU and the U.S.

As you probably know, these negotiations have taken place for a very long time, and there were a lot of contentious issues that the delegation successfully resolved. Notably, the judicial redress legislation that is pending in Congress right now has been a long time ask by the Europeans.

And the administration and members of the interagency worked very, very hard to craft judicial redress legislation that meets the needs of the

Europeans, accommodates the interests of the Federal Government, and reflects the administration's commitment to answering this ask by the Europeans.

The Privacy Office staff worked very hard to support our involvement in the interagency talks with the commission. Just to provide you some context, the DPPA will serve as an umbrella agreement with baseline standards for protecting PII exchange for law enforcement, criminal justice, and public security purposes.

Although it has been finalized, it does not go into effect until the judicial redress legislation is actually enacted. We await those developments eagerly. It is anybody's guess what Congress will do.

But again, the conclusion of the agreement represents years of very hard work, including enormous work by my staff. They are to be commended for that.

I want to talk a little bit about the compliance work that we have done. Compliance is a busy 24/7 function within the Privacy Office. Since

our last meeting, the DHS Privacy Office published 45 PIAs and 26 SORNs. The office has been very focused on biometrics and information-sharing.

As DHS transforms its management of biometrics from a component-centric to an enterprise- or DHS-wide approach, the DHS Privacy Office has and continues to promote policies and decisions consistent with its 2011 privacy policy guidance memo on IT-shared services. The way we are handling biometrics is sort of envisioned to fall squarely within that guidance.

The identification of stakeholder roles, such as a data steward, a service provider, and data user, are informing DHS's development of an enterprise vision for biometrics. These roles and the underlying policy considerations for their identification inform not only the manner in which biometrics are and will be acquired and maintained but also the manner in which biometrics will be used and shared with DHS partners.

The recently released DHS biometrics strategic framework 2015 to 2025 reflects this

initiative and the Privacy Office concerns in two specific ways. First, it establishes an objective related to elevating biometric privacy compliance from the component to the enterprise level, as I indicated, and emphasizes categorizing information according to the purpose for the original collection, and sharing it for compatible purposes, and promulgating another objective directing the creation of an internal DHS governance structure to prioritize and manage biometric portfolio objectives across the department to preserve the role of oversight organizations, such as the DHS privacy, civil rights and civil liberties and the Office of General Counsel, to ensure the execution of a strategy while continuing to protect the rights and privacy of citizens and operate within relevant legal authorities.

As the governance structure is established, the Privacy Office will continue to remain an active stakeholder and participant.

Many of you are familiar with our data framework, as you have given guidance to us in

response to a number of taskings. We continue to expand significant resources on developing the data framework with our colleagues in the Office of the Chief Information Officer and the Office of Intelligence and Analysis.

Recently, the department's leadership made the decision to accelerate the movement of data sets into the framework with the goal of including up to 20 data sets by the end of fiscal year 2016. So that is a pretty aggressive acceleration schedule.

Faced with a critical mission need to perform classified clearings on unclassified data in order to identify individuals supporting the terrorist activities of the Islamic State of Iraq and the Levant, al Qaeda in the Arabian Peninsula, the al-Nusra Front, and affiliated offshoots of these groups or individuals seeking to join the Syria-Iraq conflict -- as you know these individuals are often referred to as foreign fighters by the media and generally in public discourse. The department adopted an interim process that foregoes many of the automated protections of the DHS data

framework, such as the tagging of necessary data sets in the unclassified data lake.

Although the interim process does deviate from the standard model of the framework, DHS is pursuing this process under the auspices of the framework in order to utilize aspects of the framework's privacy policies, governance, and transparency. The interim solution will only continue until the standard model is capable of meeting the mission need, this particular mission need as well. DHS remains committed to the standard model of the data framework for meeting our mission needs in the long term, and the department will revert to the standard model once the technical capabilities are available.

Consequently, regular development on the framework will continue and will not be affected by the use of the interim process.

We published a PIA to address this exigent circumstance and be transparent about it. The PIA was published in April of this year and is available on our Web site.

While I am on the topic of the data framework, I want to talk a little bit about the recommendations, the most recent recommendations you made. While our attention and resources have been somewhat diverted due to the acceleration and exigent scenarios, we have taken to heart your recommendations, particularly on transparency and auditing, that you provided at the last meeting.

With respect to the transparency recommendations, we in the Privacy Office are in the process of developing a dynamic public-facing Web page to provide as much transparency as possible. I personally really very much appreciate the recommendations on transparency in the context of being dynamic. I think it is very important, and it is important to recognize that although our PIAs are model PIAs, there are other ways that we can reach the general public and others who are interested in our activities.

The Web site will create a living document that provides ongoing updates and reports to the public on material changes to the data framework.

The Web site is a priority for fiscal year 2016, and I hope we can provide you with frequent updates on its development.

While I am on the topic, I should say that I consider your recommendation, although it was provided in the context of the data framework, I think your recommendations on transparency were exceedingly valuable to transparency writ large within the department. So I thank you for those recommendations and appreciate the work you did to formulate them.

I just want to emphasize that we are committed to addressing each of your recommendations, and we look forward to sharing details, as I said, about the progress we are making. So don't be surprised if you hear from us during the course of the year.

Before I wrap up and kick this over to others, I do want to spend a little bit of time talking about FOIA and our activities on the FOIA side of our house. I did mention briefly our backlog reduction. I do consider that to be great

news.

When I testified in Congress, I found myself in the position of highlighting a very small percentage number in the sort of downward trend in the reduction. Because I am an optimist and want to highlight the positive, I had indicated that although the number was not where I was going to hang my hat and rest, it was a trend in the right direction. That turned out to be absolutely correct.

As I indicated, preliminary numbers do suggest a significant reduction. All the components continue to employ a multipronged approach -- really thanks to Dolores and James -- to clearing out the department's backlogs for the use of targeted contractor support, student interns, and additional resources.

In March 2015, the Privacy Office reaffirmed the department's commitment to openness and transparency by issuing a new policy, a policy memorandum during the reporting period called Freedom of Information Act and 2015 Sunshine Week,

which highlighted some of the department's accomplishments over the past year in furthering its openness and transparency initiatives.

Also in March of this year, the office hosted an open forum meeting with representatives from components, the Office of Government Information Services, and several members of the requester community to discuss the department's FOIA processes and ways to improve those processes.

In April of this year, we redesigned the FOIA library so it will be more useful. It now includes libraries for the National Protection and Programs Directorate, FEMA, and the Transportation Security Administration, making it easier to locate records disclosed by these components.

In July 2015, I am pleased to say that the Privacy Office, in partnership with the Office of Chief Information Officer and the Enterprise Systems Development Office, created a new mobile app. This app expands the online request process, making it available to mobile devices. The eFOIA app, as we call it, is now available and through which

requesters can submit requests and check the status of existing requests any place, any time, on their mobile devices. The mobile capabilities of the eFOIA app will greatly enhance the user experience and provide convenience for the requester community.

Key features include the ability to submit a FOIA request to any DHS component; check the status of requests; access all of the content on the FOIA Web site, including the FOIA library; and receive updates, changes to events, such as stakeholder meetings and conference calls, and recently published documents.

Finally, the DHS Privacy Office is one of seven agencies participating in a 6-month pilot as part of the administration's open government initiative. So in August 2015, just recently, we began conducting a 6-month pilot to test the feasibility of publishing online the records to be released to individual requesters under FOIA, except those that fall under the Privacy Act. Basically, a release to one person will result in a release to all.

That concludes my report highlighting some of our activities since we last met. I want to thank you again for joining us. If there is time at the end, I would like to open the discussion up for a few questions.

But before we proceed, I want to welcome and introduce two of our new privacy officers, Jamie Danker and John Connors, to discuss their positions.

So welcome, Jamie and John.

MS. SOTTO: I just want to remind everyone, if you have a question, please put your cards up. Thank you.

MR. CONNORS: Ladies first.

MS. DANKER: I knew you were going to say ladies first.

MR. CONNORS: I want to be polite. If this goes as planned between Karen's talk and yours, I'll be good.

MS. NEUMAN: So let me just formally introduce John Connors, the new privacy officer at CBP, and Jamie Danker, the new privacy officer at NPPD. We are absolutely delighted to have you as

part of our privacy infrastructure here at DHS. They are awesome privacy professionals, and I will kick it to you guys. You decide who wants to go first.

MS. DANKER: He says ladies first, so I will go first, and I will yield the rest of my time to you.

MR. CONNORS: Thank you kindly.

MS. DANKER: So I am new to NPPD, but not new to DHS. I have actually been with DHS for about 7 years, 1 year as a contractor over at the DHS Privacy Office, where I worked on information-sharing issues. I quickly converted back to Federal service and was an associate director for compliance and worked on Privacy Impact Assessments, System of Records Notices. And then I developed the privacy compliance review framework, which I am really pleased to hear Karen talk about all these QCRs that the office continues to do. It was kind of my baby, so I am really glad to see it is having an enduring impact.

Then from the DHS Privacy Office, I spent

2 years over as the verification privacy officer for E-Verify, where I got to work really, really close with the programs, working on the full range of privacy issues, including their launch of a citizen center service. I got to combine some technical skills with privacy skills with that.

Then one of the questions Karen asked is how I came to this role. I was approached by the former privacy officer for NPPD who was looking to move and asked if I was interested. I thought, you know what, yes, I am, because NPPD is a very interesting, challenging place. So I did an interagency transfer in May and was very fortunate to have inherited a very well-structured office with an awesome staff, who are all sitting in the back row there. So I am very lucky to have them.

Deputy Director Diane Carr just joined that role back in May as well, but she had been with the office for the past 4 years. Cindy Falkenstein has been over at CS&C really keeping an eye on all things cyber for the past 4 years, so she is my eyes and ears over there. And we have James Burd, who

just joined us recently, formerly at USVISIT, and Scherida Lambert, who does lots of things, keeps track of all our taskers, privacy incident management. And I am not going to forget Brad Bartel, who really is sitting in the back row back there, who also has one of our Office of the Undersecretary positions. So I am really, really lucky I have a team of great, great privacy professionals.

We are focused on compliance. We are focused on oversight, incident management, and lots of special projects.

So I have 12 years now, a little over 12 years of Federal service. I actually started my Federal career at the U.S. Government Accountability Office, and I worked on the information management team over there. And one of my first exposures to privacy was an audit of the secure flight program. I also audited, actually, the DHS Privacy Office. And here I am now. I really believe in the office and the function of privacy, and so I came over because it was very challenging and it is very nice

to walk into an office that has a great staff to begin with.

That said, we are looking to fill some positions. And when we are fully staffed, I am excited about all the great things we are going to be doing. We are really focused right now on cyber.

We have a lot of work on automated indicator sharing. We are also looking forward to the next presentation on what is now termed AA, sort of an unfortunate acronym.

[Laughter.]

MS. DANKER: But it is very interesting. I find that, too, one of the challenges walking into cyber is that as a privacy person, you definitely have a visceral reaction to certain words, like the word "score" or "behavior," because I think most people in the public automatically associate that with behavior of individuals.

So we often struggle with that on our team. Do we rename the topic? Or do we try to focus folks on what it is that the program is actually trying to do? That is one of the big

challenges we have, trying to help ID them as customers, our cyber customers, communicate what it is that they are trying to do without raising unwarranted alarms but also raising issues that, if there are privacy impacts, we want to raise them and try to mitigate them the best that we can.

So I will yield my time to Mr. Connors, unless there are any questions.

MR. CONNORS: Well, thanks. Good afternoon. My name is John Connors. I am the CBP privacy officer. Not really new anymore. I started in July 2014. I came on right with the USIS data breach. Thank you very much. Welcome to the party.

Little bit of my background. I started with the legacy customer service back in 1992. Worked as a field person for 9 years. Decided to go to school at night. Got that law degree thing. Came down to Washington. Played enforcement lawyer for a few years. Sought my fortunes in the private sector. Decided, no, if they are guilty, they are guilty. Returned to CBP.

They said welcome back. You are going to

go into this thing called privacy in 2005. What is this? What am I getting into? At the time, it was Larry Castelli, you might be familiar with him, and Mary Beth McLaughlin. There were three of us. And it was like here you go, let's start.

DHS gave us some guidance at CBP. They said you have to do it different. You have to make it better. So we began there. Worked with Larry for about 5.5 years. Foolishly went back to the enforcement side for CBP. Worked there for probably about 4 years in the operation and enforcement side.

I guess late last year at the direction of DHS, CBP sort of changed the infrastructure on how it was dealing with privacy. We are moving it from sort of one office that dealt with it for as long as I can remember into our commissioner's office, which is the lead office within CBP. They found my name and said, hey, we understand you know little bit about this. We would like you to come here. So the joke is I was voluntold, but to be fair, they did ask.

So we are sort of in a transition,

probably about 3 years now. The old group of folks at CBP that did a lot of our privacy work throughout the years was a block of attorneys in one of our offices. As I said, DHS thought we could move that away. When we decided to make that away, we realized we were going to lose those attorneys and their skill set. So as they sort of supported us in this transition period, we have been hiring a lot over the last year. Recently, I think in the last 6 months, we hired eight folks, several fine individuals. DHS privacy has gladly shared some of their employees with us, much to their pain.

Kate Claffie is a pretty popular name in the industry. She came over and is helping me. Kathy Giove from ICE joined us. And Tony Johnson from TSA is part of our team. We continue to expand. I am currently in the process of hiring four to six more. There are some more announcements.

The numbers sounds large, but CBP has a massive portfolio. I say that in the most polite way. The volume of data that we move through the

border, the amount of data that we collect, the systems that we are operating, the sharing of that data, data framework, the international sharing of data. Information-sharing has been one of CBP -- we have been doing it for as long as I have been around. Reviewing the MOUs, making sure the safeguards are in place for when this data is shared, making sure of the accounting, putting the guards on the third-party agencies who get the data. Just because you have CBP data, you are not free to do whatever you want with it.

On top of that, with the expansion of new technology for biometric collection, we have facial recognition pilots going on.

So the mission and what we are doing, if I thought about it, I probably would have said no, I am good right where I am. But nevertheless, here I am today.

So we continue to expand. Some of the big initiatives we have are the IT expansions. Our operation folks, they are aggressive. They have foresight. They have great ideas. Sometimes when

we come in and point out that those ideas require some legal compliance before you go that route, we get a little pushback that this is really important. Everything is a national security issue.

But there is right way to do it, and that is part of my team's mission. We want to reestablish the fundamental privacy foundation element within CBP, so we are not a discussion after the fact but we are in on the discussion at the beginning. When these new IT systems come into development or changes, they are inviting my team into the room in the beginning.

We have had good luck. There are some initiatives that are ongoing that they said wait a second, let's get my team in there, and we can tell them where they are going and where we would like to go.

We have had good communication with DHS. We reach out to them on a fairly regular basis to make sure as we are growing and developing and evolving, we are doing it the way the department needs us and the way we want it to be.

So that is it in kind of a really fast nutshell.

Any questions?

MS. SOTTO: All right. First, I understand we are having some phone problems, so those of us on the phone, just bear with us.

Sandy I think emailed to say that we are working on it. Maybe we can move the mike closer.

MR. RICHARDS: Actually, that is for the transcript.

MS. SOTTO: Okay. It is what it is.

MR. CONNORS: I should have talked slower.

MS. SOTTO: No, no. It's fine.

Apologies to those of you on the phone.

Questions? Any questions from members of the committee?

I have one. It sounds like Shannon did a bang up job in her PNR work, and I am wondering if the Europeans did a similar exercise to figure out how what they are doing aligns with the agreement. And if so, how did that turn out?

MS. NEUMAN: Well, the short answer is no.

They are very focused on what we do. And we are using their information. So their interest is in really seeing how closely and how carefully we are adhering to the requirements of the agreement. So long answer, short answer, no.

I do not know if you have anything to add.

MS. RILEY: No, I think that is the right answer. We are waiting for their report that we expect we will get in the next couple of months.

MS. SOTTO: And are there substantive obligations?

MS. NEUMAN: Well, they are not using our PNR, so we are not scrutinizing their handling of it. The report is going to be very one direction. It is going to be focused on what we are doing right, what we are doing wrong.

I can tell you that the tone of the review was surprisingly positive. I mean, Shannon did an incredible job. I wish she were here. She has been told by numerous people, including the Secretary, that she did an incredible job under Kellie's supervision organizing these briefings, which were

very in depth.

MR. CONNORS: We had a lot of communications, a lot of documents going back and forth.

MS. NEUMAN: Right. And organized very in-depth presentations that were extraordinarily transparent. The Europeans were really humbled by the seriousness with which the department clearly takes adherence to the PNR agreement. They commented numerous times, even the most hostile -- there were a couple of, shall we say, not so warm and fuzzy folks on the delegation who could not help themselves. They said, wow, you are taking this really seriously. We are really impressed.

And the other thing that impressed me is how badly they wanted us to help them help us, because they have their own regulation that is making its way through Parliament and they want to tell a good story about how the U.S. uses PNR and that PNRs are a very valuable tool in the current threat environment, and that it can be used in a way that safeguards PII, and we have not been abusing

it.

So they want to help us tell a good story, so they asked us a number of questions. We had a few get-backs for them.

Now, I almost do not want to say this but I am going to say it anyway. I expect a favorable report. That is what I did not want to say, because you never know. We were in this very room together, having a very frank and friendly conversation. They are going back to their own political environment, and who knows what will happen between the review that took place here and the conversations we had here, and the conversations they are having over there.

But on the merits, I would expect a good report. On the politics, who can tell?

MS. SOTTO: How does this link with the umbrella agreement?

MS. NEUMAN: In two ways. The first link is that during the course of discussions, the negotiations, they tried to link the PNR agreement to bring it within the umbrella agreement. We

succeeded in, if you will, grandfathering in the agreement so that those protections and the adequacy finding remains.

And the other link is that there is a review in the umbrella agreement of any subsequent agreements. And the umbrella agreement acknowledges that any built-in reviews that are part of the existing agreements like the PNR agreement, and a similar Treasury Department agreement, the findings of those reviews will be noticed for purposes under the requirements of joint reviews under the umbrella agreement, so you do not have to reinvent the wheel.

They are really different, and we tried to make sure that the PNR agreement did not get sucked into the umbrella either in the course of the discussions, the negotiations, or just that it was not confused in people's minds, because there were two very separate agreements.

The umbrella agreement is really a law enforcement, terrorism, information-sharing tool. And the PNR agreement is really entered into to clarify some ambiguity about international law and

the ability to comply with U.S. law without being fined by the Europeans for providing PNR information to the United States.

MS. SOTTO: Thank you.

Okay, we are delighted to welcome Kellie Riley, senior director for privacy policy and oversight, and Jeffrey Eisensmith, chief information security officer, who will provide us with a briefing on privacy incidents.

Please proceed.

MS. RILEY: Okay. So good afternoon, everybody.

What we want to do is briefly talk to you about privacy incidents this afternoon. I am going to give you a short background of where we have been, what we are governed by in terms of our response in privacy incidents. And then Jeff is going to provide some information about recent events, recent breach incidents that we have seen, and kind of what is maybe different about those or just how they impact us moving forward.

Following our briefing, we are really here

to set the stage a bit for the tasking that Karen will provide at the end of our briefing. We are happy to take questions once we are through here.

Generally, when we talk about privacy incidents, the documents that we look to in responding to privacy incidents are documents that most of you are likely familiar with. We have OMB memorandum 716, which was issued in May 2007. There is also the OMB memorandum without a number that is called Recommendations for Identity Theft Related Data Breach Notification, which dates from September 2006. We implement those here at DHS through our Privacy Incident Handling Guidance, which we fondly refer to as the PIHG. We even have little squishy pigs hanging around the office.

In the coming fiscal year, the Privacy Office is planning to embark on just re-looking at the PIHG in light of what we have seen in terms of incidents and trying to determine if it still works for us. Are there things happening that we need to address in a different way, including things like individual notification? Are we doing all of that

in a way that makes sense, given what we are seeing currently in the incident arena?

The documents that we look at, these documents that specifically address privacy incidents, contemplate a variety of types of incidents, both those involving information technology and also paper-based incidents that are not IT-system-based.

The focus of those, though not exclusively, is on employee responsibility and our obligations as individual government employees to protect personally identifiable information and how we must respond to incidents when they occur.

I also want to note in addition to the documents that I have referenced, there are a variety of security NIST and FISMA requirements and internal security documents that are more focused in Jeff's arena. Just a few, probably this high. If I tried to name them all, I would get the numbers wrong.

So we have a variety of things that we are looking at. But the ones that I referenced are

privacy-incident specific and PII specific.

Much of the current incident handling guidance arose out of the famous 2006 VA laptop incident. That was my first foray into privacy incidents and maybe the first foray of a lot of government employees into privacy incidents. Most of you are familiar with that, a stolen laptop, not encrypted, millions and millions of veterans' PII contained on that.

And that is not an uncommon type of incident in terms of what the bread-and-butter of our privacy incident group sees on a day-to-day basis. Only now when you lose a laptop, because we addressed that back following the VA incident, if you lose a laptop, it is usually encrypted now, or by policy, it should be encrypted now. So the mitigation is different and how you have to respond to that is different.

But we still see laptops get lost. Blackberrys get lost. Thumb drives get lost. People send PII outside of the DHS firewall without encrypting it, or they send it within the DHS

firewall in violation of a component or office policy that requires it to be encrypted.

Interoffice mail gets lost. A FedEx package gets lost that contains PII or sensitive PII.

Sometimes we see shared folders on our network that should be more locked down than they are. Someone gets in and says, "Oh, I probably should not be in this folder." And we have ways to go in and fix that.

But a lot of those incidents are about what the employees have done. They are accidents. They are mistakes that they have made. They are addressed through policies and documents that talk about how you handle information. There are ways to mitigate the risks that those incidents pose by tracking documents, pulling them back. Someone posts something publicly that should not have been posted. We pull it down.

So generally, we are taught the bread-and-butter incidents are these accidental, no malicious intent, usually things that happen. And we can deal with those through counseling and policies that we

have.

The risks that we generally are concerned about when we talk about sensitive PII, or generally have been concerned about, are identity theft and what is that information that was breached, what can be done with that information, and how do we help the individuals who were affected deal with the potential implications of that? That is a progression, and it all stems from what happened with the VA. Shortly after the VA, the Bush administration had the President's identity theft task force. These OMB memoranda came out.

Now that is not to say that the documents that we have in place do not contemplate some different kind of incidents. Our PIHG, for example, requires when someone is reporting an incident to tell us what the incident category type is. These can be an alteration or compromise of information, misuse, unauthorized access. These are things you think about in big IT systems, but they are not the everyday, or have not been the everyday. We hope they do not become the everyday.

But as IT systems progress, and bad actors get more sophisticated and are looking for more and different kinds of information, we see different things. Like I said, I hope it is not the norm. I hope it is not the day-to-day, but we have seen enough. I am going to turn it over to Jeff, and he is going to talk about sort of the more recent big incidents that we have been faced with, and let you know a little bit about that. And then we will take questions, and we can talk about where we are going from here.

MR. EISENSMITH: So if you have questions while I am going, I have no problem with just you raising your hand and saying, "Hey, you." Whatever you want to do, that is fine.

Let's start off with the just the scope and scale of these breaches. It is kind of mindboggling.

When you look at the OPM breach, 23 million was the count. This was very invasive data.

This was data that involved background investigations. So it does not get much more

personal than that, because it says where you traveled, who your relatives are, how often you go to that place that is outside the country. You can almost think of it, for those who are old enough to remember what a Rolodex is, the adversary is building of Rolodex of all of our personnel so that when they are in a place and time when they need something to happen, they can say that is the person in the chair that affects that. Do I have them in my Rolodex? Yes. Then, by the way, the background investigation, in the notes, they were able to get that the guy always does this. I might be able to leverage this, and then leverage that person, whoever he or she is.

So from that perspective, we know that the adversary has an appetite that is insatiable for this type of information. And you are seeing it broad brush in both the government and the companies that work for the government, and now in health care as well, so extraordinarily broad.

One of the things we are finding as we look out across the environment is a lot of the

companies that are handling PII, excessive PII, have grown up in a world where it started off with FedEx.

You do your paper form and put it into a FedEx and ship it, and the investigator tears it open and goes door-to-door and fills this thing out. And over time, organically, they grew into an IT unit, so we can do this faster and cheaper, have higher profit margins if we begin to introduce the IT world into this.

I can tell you from my experience, IT does not grow well organically. It does not. It has to be carefully planned and manipulated and kept in a box. So we are trying to recover from those sins.

The big thing we are doing right now, there was a great partnership between privacy and my office and procurement. Let's come up with contract language -- this is not the name for it. It is just what I call it, the cyber hygiene clause. It says let's relook at all these contracts and identify if they are processing sensitive information. And if so, how do we get a better handle to not go through the sins of the past? What was Einstein's

definition of insanity? Doing the same thing again and again and again and expecting to get some different outcome.

So to break the paradigm, we want to go into all of those contracts out there and bilaterally negotiate in the clause. And the clause is a new way of doing business. In the government world, we look at the sensitivity of the data and we classify it under three categories CIA, confidentiality, integrity, and availability, CIA. In the NIST world, it is called that is called a FIPS 199 categorization. It is usually mod, mod, mod, or high, high, high. But if it is a mod, mod, mod, or a high, high, high, NIST has a cookbook that you just tear open the page that says high, high, mod, and these are all the controls that go along with that.

So in the contract, we basically say here are the controls. You have to implement these in order to authorize your system. And then the government will recognize that authorization. This is a big paradigm shift. If we recognize the

system, then we will allow you to do the work and ingest our data.

But there are a couple caveats to that. One of them is while you put these controls in place, you must have an independent third-party come in to assess those controls. And then you are never completely done. No system is perfect, at least not one I have seen in my entire career. There is always, "I am 95 percent there. I have 5 percent residual. I will get to in 6 months." That is called a plan of action of milestones.

As an organization, DHS will look at this external company and make a risk decision. Is the risk low? If so, off we go. But we are not done. The sins of the past. We know that over time, if you are not watching, systems degrade. "I am busy on this" and, oh, by the way, no one ever calls the helpdesk to say, "My computer is running too fast, and I have too much functionality." It never really goes down that way.

What you are asking an organization to do is focus on security at an opportunity cost to their

business line. So in order to make that work, you have to get onsite and do inspections. So the clause calls for us to get continuous monitoring feeds on a monthly basis, and we do inspections where we land onsite and re-verify that the controls are where they should be. We are going to spot check. We are going to cherry pick. If we think there is a problem here, we will look at those controls.

Then the last piece of this is, if there is an incident, the clause gives us the right to pull chocks and come in with an incident response team and do what needs to get done, without having to ask, "Mother, may I? Can I do this?" It is signed off in the clause.

It has been a little difficult to bilaterally negotiate that in, as you can imagine. However, all new work, if your option is walk away from the business opportunity or sign the clause, they are all signing the clause. Of course, they pass that cost on to us. That is all part of due diligence.

So that was a lot of talking from me, and I understand that the way this is supposed to go is that they can ask questions and I am here to answer, so I will go ahead and throw it back to you.

MS. RILEY: Before questions, I am just going to add, related to the cyber hygiene clause that Jeff is talking about, in addition to all the security requirements that he has talked about that we do put in, we also have in that clause provisions for if there is a privacy incident, setting up credit monitoring and providing notification in conjunction with the government, so that they would not go out and notify before we knew what they were going to do and what we wanted the notification to look like.

But it is built into the contract now, so there is not a question later of who pays for this and how does it all get set up, which is important moving forward, so we know we have something in place and some obligation in place. It is not even necessarily an adjudication that something was done wrong, more that if there is an incident, we are

ready to go.

MS. SOTTO: Would you be able to provide some of the template language?

MR. EISENSMITH: It is under review. My understanding is it is extraordinarily painful getting any type of new procurement language codified, but we are doing that now. We are actually trailblazing here, getting this out. I know DOD tried, and DOD is a big beast, and they got some of what they wanted. We went for everything, and we are going to stay the course.

MR. CONNORS: I will just add one thing. The cyber hygiene language DHS put together was before the latest breach. We were working on that.

MS. RILEY: So, Lisa, we can check on what we are allowed to release, but I do know that we are working on an FRN right now as Jeff referenced to sort of go out for public comment. But let me find out. I do not want to commit without making sure what I am allowed to release.

MS. SOTTO: No, no. It's fine.

Jim?

MR. BYRNE: Thank you.

So am I to understand that you will be requesting in this clause coordination with the contractor or subcontractor notifying affected persons, meaning that affected persons would be getting notification from an organization, a sub, for example, that they have never even heard of?

MS. RILEY: So that is exactly why we don't want them just going out and doing notification. It says "in coordination and at the approval of the government," or something like that, so that we would have some ability to make sure that when these notices are going out, they understand who they are coming from and what the information is.

We do not want them to get a random notice, because people throw those away.

MR. EISENSMITH: Plus the other part of that is, we want to ensure that the protection provider actually has the chops to not -- and there will not be a second spill.

MR. BYRNE: Right. So it is likely you

would use DHS letterhead to make these notifications?

MR. EISENSMITH: That is TBD.

MS. RILEY: Yes, I think it is to be determined based on the context. And I think the potential is that different incidents will require different types of notification, or that potential exists.

MR. BYRNE: And the reason I am asking is that I would suggest that the affected person would expect that it come from the government. They have a relationship with the government. They don't have a relationship with the subcontractor that they have never heard of.

MS. RILEY: I think that is in most instances absolutely right. That is why we have it in there, and that is why we want to make sure that we are not by contract putting a requirement on them that has the contractor go off and do something without consultation. We want to maintain our ability to meet our obligations under things like 716 and our internal guidance to ensure that it is

meaningful notification and it comes from the right source.

MS. McNABB: Can a question come from the phone world?

MS. SOTTO: Not yet. Can we take everybody in the room first, Joanne?

MR. CONNORS: I will just add to that. With the breaches we had this year, we had multiple scenarios where one came from DHS and one came from the subcontractor or vendor. So there were lessons learned, is the best way to put it, and it is evolving.

Getting the communications to the affected universe has been challenging at times, how to get the message out. At CBP, we got a lot of interesting feedback on how we get the message out.

MS. SOTTO: We are going to turn to phone questions in just a minute.

I would like to just go around the table. We have, Joanne, quite a number, and I am sure you are not alone in wanting to ask questions over the phone.

Josh?

MR. GALPER: Just a quick question about the boilerplate language, because I do not think it was necessarily touched on. What about the middle ground type of finding that DHS might find about flaws in security and requiring the entity to actually fix it in order to continue the contract? So not the data incident situation where something has happened or something is happening or suspected, but you are finding flaws in security through the audits that you are probably requiring as well. Are there those next steps putting requirements on the private entity?

MR. EISENSMITH: So there is no 100 percent security. And day in, day out, it is all about making a risk-based decision. So that answer would depend on, are we dealing with extraordinarily sensitive but unclassified information? Our tolerance for risk would probably be greatly reduced. If it is something that just barely crossed the threshold, we might give them a lot more latitude.

And this really speaks to, when you open up that cookbook as to how you meet the mod, mod, mod, an NIST has 300 controls you have to meet. They do not tell you how to meet the controls. They just say you have to meet the controls, and this is the bar you have to cross.

Quite often, what will happen is there will be a negotiation that occurs. The vendor will say, "At the price point, I can give you that answer, but I will get you 90 percent there, but not 100 percent. But I have real cheap compensated control that when you combine the two should, in fact, make it." So there is a lot of horse trading that goes on that way, or I would expect a lot of horse trading that will go on that way. That is what I do now.

And the final adjudicator will be whoever is the authorizing official who owns that data. They will make that risk-based call in conjunction with privacy, of course, because, well, this is privacy data.

Does that help?

MR. GALPER: Yes, it does.

MR. PIERSON: So back to the beginning. Under the OMB guidance, right now, it is still classified the first point of awareness is into US-CERT, right?

MR. EISENSMITH: It should be your first call.

MS. RILEY: Right, right.

MR. PIERSON: So I am actually interested in that. Something comes into US-CERT within the NPPD area. So stuff comes in there. The different components within DHS, how are they being alerted to items coming in from agencies under DHS control? How does that process work in terms of alerting to US-CERT, agencies outside the DHS? So that is kind of question one.

Question two is at a super high level. Could you give a minute or 2 on the DHS Privacy Office involvement with the OPM breach in terms of what roles you played in terms of advice and guidance and that type of thing. But once again, you can probably go on for days on that. Maybe you

are more on the second question. But on the first one, I am interested in the US-CERT alerting and tie in with the privacy officers.

MS. RILEY: So the US-CERT notification happens but also for DHS components within DHS, we have a process and an incident reporting system in our security operations center. They all go through there and then get put into -- I view them as kind as separate. US-CERT, they have a different role than sort of incident response that happens within DHS.

Jeff, jump in, if you want.

But it is sort of two different roles in the incident. So we have one internal DHS process to make sure that the privacy officer see it, and everyone who needs to see it sees it. My office and my group, every incident that happens in DHS and a component is in the IT system that we use. We track all of them. Nothing closes until the Privacy Office looks at it and says okay you have done all the appropriate mitigation and counseling and whatever notification needs to happen. And then US-

CERT does their job.

MR. EISENSMITH: So it is very clear, and it is very key that you understand clearly the difference between the US-CERT and the DHS SOC, Secure Operation Center.

US-CERT is an externally facing entity that is a resource to the Federal Government, and it is also a resource to the private sector. So if something really big happens and OPM needs their assistance, they will jump up and fly. The same thing with, say, Company A, the same thing occurs.

So I run the internal shop. So think of it as big C, which is Federal Government cyber, and then there is little c, which is the department. Not so little.

So what you will find in the cyber hygiene language -- and, again, that is just our internal name for it -- is a company that is operating with the clause in effect has an obligation to notify us if they suspect something is going on.

So the way things escalate is as someone that operates a SOC, you might see 700 things that

happen in any given day, and through a process of prosecuting every single one of them, you only end up with one that you declare. This is a positive, and go down the rabbit hole.

Once we declare, I have 1 hour to get to the phone and talk to US-CERT and say that we just declared on X. That is the way this thing is sequenced.

Actually, prior to that, there is a lot of work getting done inside the department and the vendor to get to a point of actually making that declaration.

So does that make it clear as mud?

MR. PIERSON: It's interesting. It is an interesting answer because then, technically, the agencies that are external but are still under OMB guidance are putting into CERT as an FYI, but then still running a separate and distinct path, but still within the knowledge -- there are linkages.

It is good to understand how it works in practicality, in terms of operationalizing it.

MR. EISENSMITH: The OMB memo is quite

clear. Across the government, you have 1 hour from the time you declare to go to US-CERT.

MR. PIERSON: But then there are still the independent processes that run for each agency and area and charter and all the rest.

MS. RILEY: Right, and 716 requires that all agencies have developed incident handling. So when I was at the FTC, we would report things to US-CERT, but then that was just reporting. I ran the incident up the chain there. We do the same thing.

Even though US-CERT is part of DHS, we do the same thing here.

Then your other question on OPM, it is OPM's breach. We are monitoring it. We are taking the information that they provide to us. We are providing it to our employees. My team has coordinated with the component privacy offices to make sure that the information we get in is going out to all individuals. We communicate as best we can with the information that OPM provides us. But there is not much more --

MS. NEUMAN: We have also participated to

some extent at different levels and throughout the Privacy Office with OPM to help sort of formulate and address policy questions on what the approach should be with these breaches.

But we have been very clear that this is not a DHS breach, so OPM, for better or worse, owns it and they are responsible for sending out notifications, although we loan our expertise to OPM in interagency and other discussions about sort of, you know, some of the policy questions associated with this.

MR. CONNORS: A lot of the policy questions.

MS. RILEY: David has participated. Jennifer participated.

MS. NEUMAN: As I have indicated, we have had a lot of participation from our level throughout the privacy infrastructure.

MS. RILEY: But, I would say, it is especially important in a breach like OPM that the communication is clear and that we do not have different agencies sort of off reading something in

the paper. Really, we need to understand from OPM's perspective what happened.

My office is in there talking to their folks, so we have had meetings and conversations, and we are just trying to maintain the communication as best we can.

MS. SOTTO: I am going to turn to the phone.

Joanne McNabb, why don't you go first?

And then we will take others after that.

MS. McNABB: Okay. Maybe we will find this out, if we are going to get some sort of copy of some part of the contact language.

Do you actually used the term "credit monitoring"? Or do you use a broader term?

MR. EISENSMITH: I think we just notification.

MS. RILEY: You know, I don't have it in front of me, Joanne. But we talk about various types of services that would need to be set up. "Credit monitoring" is probably used, but I think there are other things included in that as well.

So I know where you are going. There are broader requirements than credit monitoring, but sitting here, I just cannot remember exactly what the language is. I apologize. I should have brought the clauses up with me. But I hear you.

MS. McNABB: Because obviously, credit monitoring is only relevant in certain kinds of data breaches. Thank you.

MS. SOTTO: Anyone else on the phone, from the committee? Committee members only.

No other questions.

Karen, I think we will turn to you for tasking.

MS. NEUMAN: Thank you. So I am going to go over this tasking. You all should have received a tasking letter from me. Lucky for you and lucky for me, I am not going to be talking at you for as long as I was earlier.

So the growth and nature of the cyber incidents make it absolutely essential that DHS has appropriate processes in place. These large-scale data breaches cannot only be very harmful, as we all

know, but as Jeff indicated, they are mindboggling.

That begins to characterize the nature of these breaches.

So protecting PII, as you know, is a national Privacy Office mission. It is absolutely essential from our perspective to maintaining the public trust and the trust of our workforce. Ensuring PII is properly used is a big part of what privacy offices do, including the DHS Privacy Office, and our voice in solving problems related to the loss and frequently, as a result of that loss, the misuse of PII is natural. It is a natural function that we perform.

It is sure to involve a great deal of the Privacy Office's time and resources these days. And incident handling is a thankless task in which there are, sadly, no winners.

Under existing Federal and DHS guidance from our PIHG, as Kellie described, when there is a PII incident, DHS is required to evaluate whether notice should be provided to affected individuals. And if we determine that notice is required, we have

to determine what the timing and content of the notice is.

As Kellie described, these materials in the past have been focused on incidents caused typically by accidental loss, such as inadequate mailing procedures, the failure to encrypt data on a laptop and, oops, leave it at the airport accidentally. But our procedures do not necessarily focus or consider the kinds of malicious actors, including state actors, that are responsible for today's cyber incidents.

So in light of the current and evolving threat environment and the changes we continue to witness, I believe it is time to undergo really a critical review of our processes. And I tasked the DPIAC today with considering whether it is necessary to update our approach to the notifications that we provide.

As the tasking letter indicates, in particular, I am asking you to consider whether we should alter the criteria we consider to inform DHS's decision of whether and when to notify the

impacted individuals. How should we compile and deliver these sorts of notices? Do we send an email out? Do we send a letter? Do we use some other platform for notifying affected individuals?

Victims have an understandable demand for information. Is it possible to overnotify, nonetheless? And in overnotifying, do we saturate affected individuals with information or bulletins?

Are there other best practices, such as structure and response teams or call centers, that you would advise?

I do not want my questions or these highlights of the tasking in any way to constrain you in your thinking. You guys are incredible experts in what you do, and we appreciate the fresh set of eyes and different set of eyes that you guys provide. So I am asking that you devote your most outside-the-box expert thinking in your guidance to us.

As indicated, these questions are detailed in the signed formal tasking letter to the DPIAC, and I look forward to exploring these issues with

you and receiving your feedback.

MS. SOTTO: Thank you very much.

What is the timing on this?

MS. NEUMAN: That is a good question. I would say, take your time and consider, except I know another incident is in the works as we speak. I say that I suspect another incident is in works. I do not have any knowledge.

So I don't know. We have not really talked through, actually, a timeframe.

MS. RILEY: I think we are hoping to review in the first and second quarter of the fiscal year, and finalize sometime in the fiscal year.

MS. NEUMAN: I think based on my experience with the committee and the subcommittee, it has been useful to have check-in calls. If you think that would be helpful, particularly after all of you huddle and sort of untangle the tasking and decide how you are going to proceed, we are available pursuant to the FACA rules and all of that.

So we think this is an outstanding

tasking, and one that taps your expertise and one that is exceedingly timely.

So I thank you. And again, happy to take any questions.

MS. SOTTO: Who will be the lead?

MS. NEUMAN: Kellie.

MS. RILEY: For now, it's me.

MS. NEUMAN: For now, it's Kellie.

MS. SOTTO: Great. I think we are really excited about this tasking. I can speak for myself.

We really have a lot of expertise around this issue. You probably have no better source of information.

MS. NEUMAN: I cannot quibble with that. Thank you.

MS. SOTTO: So thank you very much.

We can take a short break. It is 2:26. If I could ask, please, for folks to be back in their seats at 2:43 or so, so we can get going again at 2:45. Thank you very much.

[Break.]

MS. SOTTO: Welcome back, and welcome to

our new panel. A reminder to please silence all cell phones and also a reminder that we will be taking a couple comments at the end of our formal session. If you are a member of the public and would like to comment, please sign up outside. And if you are on the phone, we will take your comments following.

Our panel is going to speak to us about DHS mobile applications. We are delighted to welcome them. Thank you for joining us. We are, of course, experiencing a mobile revolution and DHS is interested in continuing to explore mobile apps for both the public and for its employees.

There is currently a draft privacy policy for mobile apps, and our panel will tell us about this and other similar initiatives.

So please join me in welcoming Kellie Riley back, and David Lindner, Robert Palmer, Doug Hansen, and Christopher Drew.

Welcome, and thank you for joining us.

MS. RILEY: Thank you. My role is really just to sit here and introduce the topic. My role

in this was to assign David this project and oversee it.

Actually, before David even joined us, we had been interested as an office in looking at issues surrounding mobile apps and the privacy issues that those involve. Many of you may remember Pete Sand, who was in policy and oversight then, but he worked in my group and he started looking at these things. Then he left us for his life in Las Vegas.

But we have done a lot of research and a lot of work in trying to figure out what is out there, what is happening within the department in terms of mobile apps, and how we can best address the privacy considerations going forward.

So David is going to talk to you about the draft policy that we have going through departmental clearance now, and Doug is going to walk you through what is called fondly around here the Carwash process and what that means from the OCIO perspective, what they are doing and how we have worked together with them to try to look at the

privacy issues.

So I am going to turn it over to them, and let them have at it, and my work here is done.

MR. LINDNER: All right. Thanks, Kellie.

I am going to start off with some background. In recent years, DHS has released various mobile apps for the public and DHS employees. The eFOIA mobile app that Karen alluded to earlier is probably our most recent app that we have released. It was actually developed by our FOIA team in the DHS Privacy Office. As Karen said, it allows you to place FOIA requests through your mobile device, check the status of those requests.

It was really important for us because it really allowed us as a Privacy Office to have an app that we could use as a test case in our very own office for how we are implementing the privacy policy we are going to talk about today.

As we know, mobile apps offer many benefits. They allow you to exchange the most up-to-date information right to your mobile device. That is important for users as well as DHS in the

field, for the employees who work in the field.

But despite these benefits, there are also many privacy concerns that are unique to mobile app technology. These concerns include the collection, storage, use, sharing of things like PII, sensitive personally identifiable information, also other insensitive information or content such as location information, mobile device IDs, metadata. And also similar to most technology, these mobile devices and apps are vulnerable to Internet security threats that could possibly compromise the user's information.

So to address these concerns, as Kellie said, we are kind of tasked with developing a DHS privacy policy and incorporate some type of privacy requirements to help mitigate against the concerns that we face.

So how do we develop the policy? The first thing we really did, and Pete Sand actually did a lot of this, was kind of conduct a comprehensive review of the mobile apps that currently exist, that DHS currently has, as was the

privacy documentation that goes with that, trying to get an idea of what our current state of mobile app privacy practices is.

After that, we also researched some industry and government best practices in the mobile app and privacy realm. The FTC has a couple good guidance papers out. The Center for Democracy and Technology also has a good paper. We took a look at those to see what we could and couldn't leverage for our own use.

Also, importantly, we worked with the Office of the Chief Information Officer, OCIO, Carwash team to try to integrate our privacy requirements into their existing process for security and testing and scans that they do. Doug will get into much more detail than me, but for the purpose of what I am going to be talking about for the policy, I just want to give a little bit of background.

So the Carwash provides development teams for the building of DHS mobile apps. It also performs security scans and tests against mobile app

source code. They have been great to us because they been able to provide the Privacy Office with the types of information that an app is collecting and using, whether or not it is accessing contacts on a phone, the photo library, the video library, are they using location information? So those are all great things that we have been able to take out of the DHS Carwash and use for our own purposes as well in implementing privacy protections.

The last thing we did is we consulted with privacy officers as well as privacy points of contact, or PPOCs, to get their feedback on the draft versions of this policy that we sent out for comment. They were extremely helpful. Most of those people, a lot of them are in the room today, provided great feedback. And we took that in, in developing our policy.

So the Privacy Policy for DHS Mobile Applications is under review right now as a management instruction, a DHS management instruction. And eventually, once it is published, it will implement our privacy policy and compliance

directive.

Just so you know, because you might have some questions, a DHS management instruction is kind of the instrument that DHS uses to explain how to implement our policies and directives. They go through a rigorous review process throughout the department. That is, currently, where we are with our own draft instruction right now.

The privacy policy that we drafted applies throughout DHS for mobile apps developed by, on behalf of, or in coordination with department. We really wanted to cover everything we could with this instruction.

We build apps internally here at DHS, but we also often will work with third parties in developing apps. There have been other instances where we have worked in coordination in some way, not fully our app, not fully somebody else's, but it has a DHS seal of approval, if you will. We wanted to make sure if we are doing those things that the price requirements that we have for mobile apps are incorporated. So we can see those apps, we can put

privacy protections in, go through the DHS Carwash process, and so we are covered as best we could be.

So as part of our privacy policy, we developed a set of minimum privacy requirements. So the first thing, obviously, provide notice, a couple different types of notices.

First, the app specific privacy policy. We ask in our privacy policy that this policy be app specific, obviously, and also appear in the commercial app store as well as within the app itself once it is downloaded, so you can constantly go back to it and take a look at what the privacy policy for the app is.

This policy, we actually give a template in our draft instruction of what things should be covered in this privacy policy. So basically, it should cover the basics of what information is collected, how the information is being used, if there is any information-sharing, app security, and also how to access and correct your information, obviously. If you are inputting information to this mobile app, you should have a way that you can go in

there to change it and request that information back.

Also, privacy statements. It is kind of a no-brainer. If DHS is collecting any type of personal information from an individual through a DHS mobile app, then we need to provide a privacy statement at the point of collection. This was most recently done in the eFOIA app. We do it a lot through pop-up notifications. So when you put in information, the app will prompt you with a little pop-up and give you the privacy statement so you have to kind of say okay when you are putting information in.

The last part is contextual notice. And, again, it is obviously all based around context. You can see up there, you will see this in a lot of apps that you have. If you update your app, a lot of times it will say if the use of information has changed at all from the previous version. We want to make sure that users know that. It is a DHS mobile app, they get alerted to that, so that they know upfront any changes that have been made to the

privacy policy.

Also, just-in-time notifications. You also see this a lot. Say you are using your phone and you click on a capability within the app and it asks you if you are sure you want to turn on location-based services. It gives you that option.

So we want users to actually consent upon the first time it is going to go in there and actually look at any type of sensitive information, or access or use sensitive information.

Lastly, independent opt-out features, this kind of goes hand-in-hand with the last one. But you want to be able to customize your app. So you do not want to use location-based services, but that does not mean you should not be able to use other capabilities with the app. So say you want to turn off location, but you are okay with it accessing some other information or that you can submit a request as long as it does not track your location, which we do not want to do. So it is just really important to have that customization feature in all of our apps.

The second thing is, obviously, and this is pretty self-explanatory, to limit the collection and use of any type of sensitive information. If it does not directly meet a DHS mission need or purpose, then we really should not be collecting any PII, SPII, or any type of sensitive information. If it is directly necessary and is going to achieve a DHS mission purpose, then we have to make sure -- and we are going to get to the compliance documentation and everything in just a bit -- but we to want to make sure that that is justified and documented in the privacy threshold analysis that every mobile app must have.

The next one, it is an important to establish guidelines for user-submitted information.

So a couple of ways to do this are, whenever feasible, use forms and checkboxes to kind of limit data collection. It also cuts down on any data entry errors. You want to stay away, if at all possible, from free-form text boxes where you can put in whatever information. We do not want PII, SPII entered unnecessarily.

Providing a review before sending function is also important. You put in all this information, maybe you put in a mistake or at the last second you decide you do not want to send this information off to DHS. You can back out before hitting send.

Again, this kind of goes back, unless absolutely necessary, avoid allowing users to just put information that other users of the app may see whether or not you see this in comment boxes. It is just too much risk of people including information that could be sensitive, could be personally identifiable, perhaps not even meaning to or knowing. But anyway we can cut down and mitigate that risk would be great.

The last one here is, we obviously want to ensure mobile app security and privacy. So the first step in doing this, as Doug will talk about, will be engaging with DHS Carwash. A couple of other things that we noted in our policy that we think are really important is that information submitted through an app, any type of personal information, should be immediately transferred to a

protected DHS internal system, something that is behind the DHS firewall where we can better protect the information. We do not want personal information that you're submitting, whether or not it is a FOIA request, we do not want that housed on the mobile device or just sitting in the mobile app.

As I said earlier, we want to protect that from any type of mobile security threats that currently exist today.

Also, sensitive content, so we're talking about location information -- I think, again, it's the best example here -- that a DHS mobile app maybe uses but does not need to collect should not be collected for any reason by the department, if at all possible.

So the best example I had is a couple months ago we worked on a boating app for the U.S. Coast Guard. And they do have the ability in that app to track location inside the mobile app itself.

But the reason they do that, which, certainly, fills a DHS mission need, is in case of a search and rescue mission, and you are out boating. Now to

mitigate that, however, and so it does not seem like DHS is just tracking boaters in the water, what the app does is that the app is localized to the mobile app for the U.S. Coast Guard and then when they need a search and rescue mission, the coordinates based on the phone's location will actually call the nearest U.S. Coast Guard Service Center. But when they call this through the Coast Guard, they have no idea where the boater is. The location information is not transferred. All the app does is show you this is, based on where the location is, this is the closest phone number for the U.S. Coast Guard Service Center.

So there is obviously a benefit for the user. They are getting the closest Coast Guard in range. And it is also protecting your privacy, because we do not have their location. The user will have to provide where they are, where their coordinates are in the water once they call into the Coast Guard to actually try to help them out. So that is a mitigation that we thought was really good and important.

The next thing I want to talk about is the privacy policy also outlines a DHS mobile app development process. It all starts with program managers and system managers who are thinking about getting ready to develop a mobile app. We want to make sure that they engage with DHS privacy or the component privacy officer as well as the OCIO Carwash team as quickly as possible so we can kind of work through everything, all the steps they will need to take to make sure that the privacy requirements as well as security and OCIO Carwash requirements are captured.

So obviously, component privacy officers will engage with program managers to ensure that the privacy protections that we outlined in this privacy policy are integrated from the start, from the very beginning. So that is our way of baking privacy in from the start.

And, of course, before any app deploys, we require that the app go through the DHS Carwash. Once it goes through the Carwash, the Carwash team will provide the scans and results back to the

program manager of the actual app, who will then work together with the component privacy officer or the PPOC, the privacy point of contact, in putting together a privacy threshold analysis that we can take a look at all the privacy concerns as well as making sure that the results from the Carwash scans accurately describe what we stated in the PTA.

So if the PTA says we are not collecting or accessing the mobile device's photos and location, and the results come back and say they are, then we obviously have a problem and we need to figure it out. Either it is supposed to and we need to justify why it is going on and put it in the PTA, or we need to make sure that those features and capabilities are turned off within the app.

So once that is all figured out, the PTA and the results of the Carwash are then sent off to the chief privacy officer in our DHS Privacy Office to make sure that appropriate privacy protections are included for this app's deployment and also to make sure there is no other privacy compliance documentation that may be needed, such as a Privacy

Impact Assessment, System of Record Notice.

And finally, once it is all determined that adequate privacy protections are built-in and that we have all the document privacy documentation that we need, the chief privacy officer will sign off on the PTA or any other compliance documentation. And the app is ready, from a privacy point of view, for deployment.

The one last thing I want to mention is that we added in that DHS mobile apps must go through the Carwash process every 6 months and as well as existing DHS mobile apps that were created before this policy was instituted must go through the Carwash within 6 months of the policy's issue date.

Obviously, here we just want to be aware of anytime there is a change to any of our programs. But in case there is a code, something goes wrong, it makes a bigger change than maybe even the developers thought it could have caused, in terms of the uses of information, we want to make sure that we have the ability through the Carwash to go in and

make sure everything is running the same. And if it is not, obviously, we need to update our compliance paperwork and, obviously, make sure that we have mitigation in place for any new privacy things that may be coming through.

I am just going to turn it over to Doug now to kind of walk you guys through a much better job than I did of talking about the Carwash.

MR. HANSEN: Well, thanks for having us here.

I just want to first address that this is a service offered by the CIO. It is a no-cost service. I want to get that out of the way first, because I am sure we will have that question. How much does it cost? There is no cost to use it.

We work with all the compliance offices. We work with those. We work with security, with privacy, and the developers to provide them best practices, lessons learned. So we provide the entire roadmap, if you would, for concept of your mobile lab to development of your mobile app, to what things they need to do to get permission to

deploy my mobile app, to actually provide -- we have the credentials to deploy in the popular mobile app stores.

So rather than figuring out how to deploy to Apple or Android or the Microsoft app stores, we have the credentials and relationships with Apple and Android and Microsoft to deploy those apps up to those environments. Plus, we work with all the other components on what app store is internal. So if it is an internal app, we can help the developers' program offices figure out how to work through how to get an app deployed.

So the big thing here for privacy is knowing what the mobile app does. Everyone looks at it and says it is just a mobile app, but it is still an IT system. It still has to go through all IT system requirements, FISMA, security, privacy, 508, accessibility. So we help shepherd those apps through that process.

For privacy, we do scans as part of our security scans that produce reports that David was referring to that allows you to see what features

are turned on because a developer who is developing from a software development kit may not know that I have to go in configure that my geo-location system needs to be turned off, or that, out of the box, I am pushing my contact information to some third party. So we help identify those things are turned on and then we help them figure out how to turn them on so that the PTA that they submit matches what their application is actually doing.

The next slide, our environment for Carwash, we provide an environment for software development so you can go in and go with your requirements and meet with your developers and manage your development team to take your source code, check your source code in. We do dynamic and static code analysis.

We also do on-the-fly security scanning. The tools that we use are both COTS and open source.

The goal is to use as much open-source because it is a free service. It is free all the way up through the COTS tool. So we will provide everything that does not have a license cost

associated with it. Our approach is BYOL, bring your own license. So as long as you bring us your license, like Fortify, if you wanted to use Fortify, it is part of our security boundary. We can use Fortify. We will only use Fortify for your application, but you have to provide us the license to actually leverage the Fortify tool for scanning purposes.

Then the reports analysis, not only do we actually run the scans but we also provide the place where you can retrieve your scans, automate that scan process so you can check it in and we're not in the middle of your process. But also, once you get your report, we will help you look at your report. If you have questions, we point you to your security officer. But we also provide best practices on how to fix this vulnerability or you have geo-location turned on and you're using this software development kit, we can help you figure out how to turn it off.

Next slide, everybody likes pretty slides, so this is our Carwash. Again, the longest pole in this process, as David alluded to, is signing up for

access to the system. So we had to get your program office, your security officer, people access to the system to get the project stood up. From time of initiation, it could take several weeks. But once that is set up, you have a time on your application and you can check your code in, run your scans, get your results. You only need to consult Carwash when there is a question or concern or the privacy is asking us a question. We try to make it as autonomous as possible.

Are there any questions on this slide?

The summary is it is Carwash, but we are trying to do application lifecycle management support for all software development, mobile being a big piece of it, but trying to give best practices, playbooks, roadmaps on how you build an app, how to make sure that my app is doing the right things it is supposed to be doing.

For example, we actually built the eFOIA app for the Privacy Office. One of the biggest learning curves we had was making Apple app compliant. So actually going in and working with

the accessibility office and making sure the colors matched, are right, the pick list had focus. So those kind of issues, we help worked with them to figure it out.

And then everything that we do provide, we have a wiki page so that we can share that information for people who are doing mobile development.

MS. SOTTO: Okay. Let's take questions in the room first.

MS. VANDERVOORT: Yes, I have a question about the sponsored apps. So all of these, I take it, are developed by contractors but they are DHS-sponsored apps?

MR. HANSEN: We can support both third-party apps, apps that are built and are out on the Apple Store that the component wants to bring into their GFE or bring into the department, or apps going outside the department. So there would be both static and dynamic testing. So a sponsored app would be anybody within the department component that either wants to use the app as internal and put

them on your GFE phones or push it out to an Apple or Android store.

MS. VANDERVOORT: Okay. So I used "sponsored" a little differently. Either way, they come under the DHS umbrella. So even if it is an external application, I as an external user would see it as DHS.

MR. HANSEN: Well, for those types of apps that are brought in and put on your GFE, you would not see it as a DHS-sponsored app. You would be redirected to a mobile device manager or a mobile application manager that your component is using. And that is how you would get that app added to the store so I could download it onto my phone.

MR. LINDNER: So a lot of times -- I know what you are getting at. A lot of times there is coordination between the third-party and the department. There is a mutual benefit a lot of times in getting an app out there. So we will provide data, and we have a contract with them, but it might not be labeled DHS mobile app or whatever, but it will have the DHS seal and it will have the

third-party's main whatever they are calling it. They will put on a logo. And if you go in the app store, it will say DHS-sponsored, worked on by DHS.

MS. VANDERVOORT: Then that gets to my next question, which is in terms of the requirements for data handling, what you described was a lot of customization based on what the app actually does. But in terms of the policy requirements in terms of collection and things like that, is there consistent -- sort of any DHS app has the same policy so that there is a consistency for the user community? Or is it app by app and function by function?

MR. LINDNER: Well, I would say that our privacy policy is that we bring minimum privacy requirements, so that is what we say right off the bat. Of course, they always have to stay in line with our FIPS and our other existing privacy policies, obviously. But in terms of when I got to justifying something in the PTA that is like a DHS mission need, it is very difficult in an agency like DHS. There are so many different missions that our operational components have that sometimes it can

be, we do approve location for this app but not this app. If there is a valid reason for it, like search and rescue, things like that, where obviously we want to help people with Coast Guard search and rescue missions. But the eFOIA app, we do not need to be tracing where people are making FOIA requests on their mobile device.

I think we did the best we could in developing a standard that all mobile apps that come through, the requirements that they must assess and implement. And if there are variations outside the box, I think sometimes you do have to look at it based on the mission need, if that helps answer your question.

MS. VANDERVOORT: Yes, it was more of a consistency in interacting with a partner.

By the way, the Carwash is really cool.

MS. SOTTO: Chris?

MR. PIERSON: First, kudos on both static and dynamic scanning. That is great. I am glad you guys are running the Carwash to make sure that gets done.

A question on future use or how you see the uses within the organization happening within DHS with the apps, especially in terms of where people do want to send more sensitive data back and forth. I think there are a number of different ways of using apps, CBP, et cetera. They are going to want to send back information that is going to be sensitive information.

What do you see in terms of organization, how does your office or how are you approaching that topic as you reach out to constituents?

MR. HANSEN: So like David said, we provide best practices and collecting data from your mobile device can be encrypted both at the data entry point through the process of pushing it back to your backend data source. It's just like any other system where I am collecting sensitive privacy information or any type of information from a Web browser or from a customer or an end user's Web browser.

So as long as we can identify that the data is protected, or if it is privacy information

being captured, that type of information can be identified, reported on, and then provide guidance on what encryption methodologies are authorized to use, how you work with your ISO to make sure that that channel is fully encrypted and fully protected, and that you are going to take into the backend data source.

So I do not want to have PII data captured and put up into a public cloud without having the right controls and everything in place.

MR. LINDNER: I think a quick answer is we are not there yet when it comes to the public. I think when we are talking about phones where it is a DHS employee using an application, there are some mobile apps that are basically the mobile app form of an IT system that they would have at their desktop.

You especially see this a lot in CBP. They use it out in the field, like they will record data like people's names. They will use that in the field on a tablet or a phone. There is encryption.

The security is all there in linking it all up and

entering it right into the protected DHS system.

So I think we are much better there obviously because we have control over the devices and all the security around it. I do not know we are really there yet on how we want to deal with -- obviously, it is a draft policy. We have taken a very conservative approach so far in what we are accepting from the public, but, certainly, what we are pushing out in terms of anything being sensitive or PII or anything like that.

I do not think we are there yet. I am not sure what the future holds. We have not had a lot of requests for that either, so we, certainly, have been basing it on what people want to do, what the program system managers have come to us with. We have not seen that yet. I am sure we will.

But I think right now, I think we are still learning, obviously, and we are going to continue learning throughout the process.

MS. RILEY: I think that is right. I think mobile is the way of the future, it seems. I think we are going to have to figure out, as we are

collecting information from the public, if we have a need to collect sensitive information, we will have to figure it out. Sometimes it is going to be making sure they understand where it is going and what the security is around it. Notice isn't perfect, but notice is notice. Then we can just ensure that it comes into us securely.

MR. PIERSON: I definitely would suggest in the future to include tokenization as a way to actually not collect data, but collect something else in its place, different from encryption of the original underlying artifact. There are obviously differences between the platforms, but they are there. They are ready. They are working.

MR. LINDNER: So that's great. Thanks for the suggestion.

MS. SOTTO: Okay, I am going to go to the phone.

Jim Adler, I know you had a question.

MR. ADLER: Yes, I think this is fantastic. My question relates to the dynamic analysis of every 6-month Carwash review. Are you

guys going to be looking back on operational data from the application on the previous 6 months of activity and doing a review of that data from an operational view to see if the operation has been compliant with the policy?

MR. LINDNER: I don't think we are there in terms of doing almost an audit of what has been performed in the past 6 months. I think it would be similar to the first Carwash we did, just to make sure all the code and everything is the same, no other features have been turned on. I think that is where we are at, at this stage.

Obviously, like we were saying before, we want to keep growing and continuing to do whatever we can to make sure these things are functioning, these apps are functioning the way they are supposed to and we were told they were going to.

MR. HANSEN: Not the data, but like David said, things could have been changed or configurations turned on. But also with new vulnerabilities that are introduced on an ongoing basis, it might not have been a vulnerability when

we scanned it 6 months ago, but it is now a vulnerability. We want to make sure that we are continuously checking to make sure that we are covering our bases on those not exposed vulnerabilities, but weaknesses that have been just identified.

MS. RILEY: And, Jim, this is Kellie. The other tool that we have, and Karen talked a little bit about this in the context of the PNR, is our PCR program. So while we do not have it mapped into a fiscal year plan yet, the option always exists for us to go in and do a PCR on one or more mobile apps and see how they are working.

So I imagine as we develop the policy and it gets in place that we will want to do that and go back and take a look at the actual operation of the app and the data and how it is all flowing. It is not built into the current policy, but it is always an option for us.

Mr. ADLER: That's great. Thank you.

MS. SOTTO: Okay. I am going to apologize to anybody else who has questions. We are running

behind, so I would like to move this along. Certainly, if there are more questions, please do submit them to Sandy or me. We will make sure that we get them to you guys and will get answers back.

Thank you so much.

MR. LINDNER: Thank you.

MS. SOTTO: For our next panel, Dan, come on up.

The committee had received a tasking on behavioral analytics in cybersecurity capabilities, which we have renamed algorithmic analytics, which Dan will explain. Our Cyber Subcommittee is headed by Dan Chenok, and he is here with us to give us a preview of what the draft paper looks like. It is in great form, and Dan is an amazing leader and very well-organized and has forced product to all of us on the subcommittee.

So the original tasking, I just want to note, was issued in September 2014. It was revised in January 2015. So there has been really quite a bit of activity, and this has been a very active subcommittee over the course of the last few months.

Dan, please take us through it.

MR. CHENOK: Sure. Thanks, Lisa. Thanks for having me. Thanks to you and Chris for being stalwart members of the committee and for anybody on the phone, other committee members.

I am happy to be joining you today. It is always great to come back to talk with the full DPIAC committee. The last time I was here was when we were issuing the Cyber Subcommittee recommendations for security and pilot projects a couple years ago. So I am happy to be back.

This is essentially an in-process briefing. We are still working on the report and will be going through drafting and final reporting, and getting it through to recommendation to the committee to Karen and your office thereafter. But because of the timing of some of the DHS work and the fact that NPPD especially wanted to hear from us about some of our thinking in this area with regard to some pilot projects that they are working on in this space, we thought it was appropriate -- is anybody here from NPPD today?

Hi, NPPD. Fantastic. NPPD has been phenomenal as almost a virtual member of the team in terms of getting us information and answering questions that we had. So as I am explaining the program, our interpretation of it, if I get anything wrong, I will invite you to speak up and correct me.

So as Lisa said, we got a letter almost year ago that came via Karen that basically talked about a phenomenon that DHS through NPPD was working on behalf of the government cybersecurity world to look at something called behavioral analytics. This concept, which I will get into in a minute, is essentially analyzing cybersecurity traffic not related to a signature or the user or a particular machine, but looking for anomalous patterns primarily in machine-to-machine activity to see if you can associate anomalous patterns with malware that you might then be able to go in and stop bad traffic from happening or find bad guys and that sort of thing. There is a lot underneath that, but in a sentence or two, that is kind of our kind of interpretation of what the discipline is.

So I am just going to go through the deck. So slide 2 gives you the definition that I just talked about.

There are two pilots NPPD has underway, LRA and AAP. These are pilots looking at this technology in different settings working with different agencies. I won't get into the specifics of them now, but DHS is being very responsible in sort of piloting the notion and then developing ideas for that before it expands. That is, certainly, good practice.

Of course, in any sort of monitoring traffic, whether it is signature-based or otherwise, there are privacy issues that come into play. That led to the request that the DPIAC through the Cyber Subcommittee take a look at what those are. The subcommittee received a number of briefings from NPPD about this. We have had some great discussions both on the phone and in person. So we are very grateful again to NPPD for providing that, and we hope that our findings are useful both to the Privacy Office and NPPD on behalf of the government.

Our approach to the tasking was essentially to try to get a handle on the scope, which Lisa referred to in terms of the title. Then we kind of took two parts. One is, what are key crosscutting considerations in thinking about protecting privacy in this particular discipline? And then at each stage of the pilot project or the program, how can you think through privacy protections at that stage? And then finally and importantly, various subcommittee members would often to bring up, "We wrote a report about X in 2012 or 2013 or 2014, and we really ought to just adopt that as a part of our recommendation for this because it was really a recommendation that would fit here." So when we do a report, we will probably have sort of a "here are the DPIAC reports that speak to this issue." We will have a taxonomy of that that we can refer to. Of course, the Cyber Subcommittee report that I referred to earlier is one of those reports.

So slide four, the first thing is the context of behavioral analytics. One of the

concerns being a subcommittee of the DPIAC and a group privacy professionals, when we saw the term "behavioral analytics," we said, "Oh, this must be about tracking human behavior." That raised lots of issues that we thought were the case.

Turns out that was not the case at all. This is really about looking, as I said earlier, at patterns, traffic patterns among machines, looking for anomalies, that sort of thing. The thing that we talked with DHS about and that we were concerned about was that if the "behavioral analytics" term was headline, that that would then lead the public into a different conversation, and it would not really get to the merits of the issue.

So we talked through what the concept of the program was all about. The term that we came up with, among several, but the best one we came up with was "algorithmic analytics," because you are really looking at all algorithmic patterns in traffic unrelated to IP signatures, unrelated to particular machines, and seeing if you can, from those patterns, develop baseline pictures and then

anomalies that can be associated with problematic activity online that DHS would then want to follow up with, with further human analysis and intervention. So that is sort of the reason behind the term.

You see that kind of laid out here in the sub-bullets. The first bullet is establish a baseline, use machine algorithms to look for anomalies. That allows DHS and the analysts working across DHS and cybersecurity offices across the government to really focus on those areas where anomalies have pointed to particular problems.

So it is, essentially, if you will, divide the haystack up from one big, giant haystack into maybe a lot of smaller haystacks where you actually think that there might be a needle there, as opposed to the ones where there is probably not going to be one there.

So that is really what this is all about, trying to make DHS and other agencies much more effective in looking more specifically at traffic patterns to determine where there is a problem.

MR. TIEN: Can I interrupt for a second?

MR. CHENOK: Yes.

MR. TIEN: One of the things that I did not quite understand from the slides was how is this approach, algorithmic analytics, different from what we have with EINSTEIN?

MS. SOTTO: Lee, sorry, can I interrupt you? Are you asking this as a member of the public?

MR. TIEN: I am just asking as someone who is -- yes.

MS. SOTTO: Lee, we are holding all public comments until after the main presentation. So we will ask for public comments after we finish the formal program.

MR. TIEN: Okay. Thank you.

MR. CHENOK: So we can talk about that in the public comment period.

So the next thing we looked at was, we tried to take a look at what is beyond machine algorithms. What do the technologies look like? It actually gets us to Chris Pierson, who took a look across the commercial landscape, because a lot of

companies that some of you may be familiar with actually practice this type of traffic analysis in their own networks now. I will try to poorly summarize Chris's erudite contribution to the presentation in terms of some of these technologies that we think can provide a little more explanation about what this really is.

Again, it is not IP-signature-based. It is not based on individual machine tracking. It is looking at anomalies, things like anomalies in authentication. Agencies have lots of systems where people are logging on all the time. Are there patterns where those logins are changing from the normal pattern? And can you relate that change to increases in malware? So you know if there is a certain type of login differentiation over time, you might look back and say here we go again with that sort of authentication change. Now we know that we might want to look for that type of malware pattern coming after that occurs.

Use anomalies in terms of monitoring transactions that are occurring over systems. As

data information is being used by agencies in the conduct of business, are there different patterns that we are seeing that again are associated with problematic activity?

Egress tracking, looking at patterns of exit out of systems. Information computing environments, software applications, service applications leave in a certain way with a certain predictable pattern often, and looking at how that egress works over time and whether there are changes in that.

Oftentimes, when you deal with machine-to-machine interfaces, there will be coupling of different accounts in terms of how those machines actually operate in practice and looking at if those come together in predictable ways. And if there are unpredictable activities that occur there, are those unpredictable activities leading to problematic behavior that DHS or system administrators are seeing? And can you tie that and use those as a mechanism to look further?

Correlation methodology is looking at log

aggregations and trying to correlate log activity with machine malware type activity, as well as sort of on the warning side, setting up rules, correlation rules and tools, that you can get an automatic warning. So I have been talking a lot about an analyst who looks at patterns to be able to see, all right, there is different pattern in a machine-to-machine interface that could be associated with malware. You could set it up so that the analyst did not have to actually see it. You could set up sort of a pattern that if you see this over time, aha, here comes that problem again. Then an alert goes to the system administrator or the SOC to give them some warning.

And finally, some sort of looking at process. Industry often uses empirical scoring. When they see these threats coming in, they will use of low, medium, high, to further assist the analyst in determining and triaging where the problem is most present.

The last thing on this page is, and taking from the last presentation, mobile devices obviously

present special issues here because the use of mobile devices creates traffic patterns in and of themselves that are different. Geo-tagging on mobile devices may create new privacy issues that are not present in other types of server-to-server, client server, or even other types of machine-to-machine activity.

And then there could be use patterns that somebody who is not necessarily identifying by an individual name or location could have a particular use pattern in using a device that could be at issue here.

So those present special privacy issues.

Chris, did I cover that about right?

MR. PIERSON: You did a fabulous job.

MR. CHENOK: Okay. So now we are just going to end with two sides, actually three more slides.

How am I doing on time?

MS. SOTTO: You're good.

MR. CHENOK: Okay.

We then looked at key considerations. The

first is, after all, privacy we want to think about how PII is implicated here. DHS has been very careful in talking with us about making sure that we understand that there is not a lot of PII necessarily that is associated with a lot of this activity, but still it is activity over networks that we need to be concerned about, the fact that PII could become implicated. So although it is likely to be minimal, there could be a case where an algorithmic analytics pattern could point to an individual account that is identifiable by signature. That has to be properly handled.

During the analysis phase, let's say the pattern happens, the analyst sees it, they have the right haystack. Then they start digging, and they actually get into more of, this machine is actually the machine where the pattern is originating from. Is it really the machine of a bad person or did they spoof an instant person's machine to do it? Then you could get into some PII-related issues there.

We thought as a committee, and in the last few pages you will see we went through a

prescriptive process, about thinking about this in a FIPS sense, and making sure that as DHS and other agencies are implementing this, that we recommend that FIPS are appropriate for this activity as well.

So that is where we referred back to our last report that we presented to DPIAC 2 years ago, which talked about how to bring FIPS into cybersecurity pilots generally, and that gets to the relying on the existing policy point.

The second point here is we have a lot of work, and I will give credit to Ramon Barquin, our subcommittee member who has really thought through all a lot of these issues around data quality and integrity. This analysis is going to create, in and of itself, information that is used over time. That information could have chain of custody issues. It could be interfered during analysis. It could itself become a target.

So the question of making sure that we look at both content analysis, and perhaps more importantly, many of these machine-to-machine interfaces create lots of metadata. Understanding

what that metadata looks like and creating rules of looking at how you protect privacy around that metadata is something that we are continuing to look at as a subcommittee.

Then I mentioned continuing to maintain the integrity of the data.

The last is something that I am sure all of you deal with in your jobs in various ways -- thinking about applying a data governance mechanism to this program, so you think about it from a data lifecycle perspective and you think about who owns the data at which point, where decisions are made, when should decisions be elevated to a decision-maker because we see a real problem. Those sorts of activities we think are important.

And then finally took a look at accountability. Joanne McNabb led our work here. This is where we took a look at how we make sure the program is working properly. It is important that these programs have an element of human oversight to make sure that the machines are not running wild or the analysts are not running wild.

So we talked about the fact that we are looking at recommending ongoing oversight, that the oversight look at how the algorithms are designed to make sure they are not collecting too much information, that the targets of the algorithms that are being selected are essentially fair, that we are not biasing toward a particular type of traffic that the government would be trying to follow the problem rather than follow a particular suspicion where there may not be evidence of a problem. How PII is treated I mentioned earlier. We are looking at recommending that the Privacy Office be involved in this oversight process as best practice.

So the last thing we did is take a look through basically the information lifecycle, which kind of has a mapping to the FIPS as well, in terms of privacy protections that we are looking at recommending to the DPIAC for presentation to the department for how you protect privacy at each stage of an algorithmic analytics program.

The first is at the collection stage, identifying criteria for what to collect through

this program, making sure that in the algorithmic analytics data or the metadata that comes in that information is stripped of PII, to the extent feasible; that it is encrypted, to the extent feasible; and that if neither of those are possible, that the maximum privacy protections are put in place around it, potentially using a risk management framework like the one from the DPIAC audit report in 2014.

Then finally, we thought it was important to ensure that notices are provided properly and to the appropriate populations around this program.

We talked about use, and obviously this is information that DHS analysts are using through these pilot programs and potential future uses. So we try to define what those uses are: protect networks, identify potential fraud. Manage Web sites is obviously one that is an important one.

We thought it would be important to recommend to DHS that different uses probably have different processes in terms of privacy protection and that it would be good to establish essentially a

process for each use with that taxonomy, including potential uses for law enforcement. I will come back to that in a second.

Then the third thing is, once information comes into government hands, it will be analyzed most likely. How the information is protected during the analysis phase is something that we thought would be important. So it is not just protection at the time of collection. It is protection throughout its analysis in a government database or accessed by government employees.

Important questions we are looking at are how this information should be shared with other entities that are looking at these issues. Obviously, I am sure you are familiar with CERT and NCCIC. There are similar government-wide tracking and surveillance operations in cybersecurity that will be important. So establishing rules for that sharing is something that we are looking at recommending.

Establishing the technical parameters of that sharing -- this is, after all, automated

information at its base. So you can imagine that there could be automated sharing as well. That will have to be drawn very carefully to make sure that if that occurs, that the protections that we are describing are built into the sharing protocols that are designed in an automated fashion, and then the oversight comes into play to make sure that they are operating as intended.

And part of that, of course, are rules for sharing outside of an immediate network protection setting. If we really see the pattern of a bad guy that becomes a law enforcement issue, what are the rules for sharing outside of the government setting with law enforcement, et cetera?

The final two, access to the information in terms of who actually gets to see it. We thought it was important to make sure that DHS think about who the personnel are who should see the information, what should the rules be when those individuals are accessing that information, and what controls exist to make sure the people you want to see the information at the right time, that there

are specific rules for how they access that as well.

Again, we referred back to some prior DPIAC recommendations on audit controls and log controls to help guide us there.

Then finally, thanks to Lisa for helping to lead this work around retention and disposition.

This information exists in time. It probably exists in much more rapid time than most other cyber security information because it is machine-to-machine analysis, but it will potentially go into a government type of database or database that government officials have access to. So we looked at that as a way to make sure we are recommending limitations, but not rigid limitations.

A lot of this information is stuff that is going to happen over time and you want to see traffic patterns. We thought it was best to leave up to the operators with the general guidance of making sure that minimization of time is a goal to leave up to the operators what that actual timeframe would look like.

And there should be maybe different

timeframes from the collection phase and the analysis phase, in that regard.

When you get to the stage of, all right, we have seen the pattern and it is okay, or we see the pattern and is not okay, here is a strategy, it is probably time to think about how to dispose of the algorithmic analytics information and the data and metadata. So what are the rules for ensuring that disposal is done properly, that copies and shared information is accounted for, et cetera? And we are recommending that DHS think about security of all this information all the way through disposition, because, again, the databases that are created by the algorithmic analytics could themselves become targets. So it is important that those databases be designed with security in mind.

Then finally to tie all this up, making sure that the oversight process include audits and periodic reviews.

So that is sort of our mid-process review.

Lisa and Chris, do you have anything else to add?

MS. SOTTO: I think this is fantastic. In the interest of time, I am going to move us along. It was an excellent overview.

I think we have time from one question from the committee. The public comment period will come in just a bit.

Any questions in the room from the committee? Any questions on the phone from the committee?

Okay, Dan, thank you so much. We are really indebted to you.

MS. NEUMAN: Can I make an observation? I just want to say that clearly all your conversations with NPPD along with your expertise has informed your thinking about this, because I think just based on your presentation, you have managed to accommodate both interests of NPPD and the department while significantly accommodating the privacy interests.

I really appreciate that, so kudos to you and the people who worked on the tasking.

MR. CHENOK: It was a great team effort.

Thanks.

MS. SOTTO: Thank you so much, Dan. It is very much appreciated.

All right, we have now come to the portion of our program where we will take public comments. We have two comments of which I am aware.

The first is from Patrick Eddington. Patrick, can you please come up to the front?

I will just note here, we are allocating 3 minutes to each member of the public for comments. We may or may not respond during this session, depending on the question and time, but we will, certainly, get back if there is an issue for consideration.

So please go ahead.

MR. EDDINGTON: Madam Chair, thank you. I am seeking clarification on something Mr. Eisensmith said this morning. If I understood his presentation correctly, he expressed essentially the view that the Federal Government will continue to use outside vendors, outside contractors, to potentially retain personally identifying information or databases that

will contain personally identifying information.

If I recall correctly, he also said that any new contracts that would be let going forward would require essentially that a clause be included that would essentially have the effect of kind of creating some liability for the companies in question. He indicated that part of the oversight mechanism, if I recall correctly, would involve a new set of DHS-sponsored spot inspections.

So I have a lot of questions there, but I will kind of zero in on the one I think is most important at the moment, and that is, is that office actually resourced to conduct the inspections in question? And then a secondary question to that, what will the actual penalties be for failure to comply?

The reason that I am extremely interested in this is that any of you who have studied the history of what happened at OPM know that the Inspector General over there repeatedly cited the agency for failing to take proper steps in order to prevent the very thing that happened. I am trying

to figure out whether or not the proposed system here is actually going to accomplish that goal.

MS. SOTTO: Okay. Is Jeff still here?

MS. RILEY: He is not.

MS. SOTTO: Okay, we will take that under advisement. We will get back to you in some form or another on that.

MR. EDDINGTON: Okay. Thank you.

MS. SOTTO: Thank you very much.

A comment from Lee Tien. Do you want to raise your comment now?

MR. TIEN: Sure. This is Lee Tien with the Electronic Frontier Foundation.

I was confused by the behavioral algorithmic presentation because I simply do not understand how it is different from EINSTEIN. It sounds like it is, but I do not really understand the difference. So I am wondering if, in fact, there is any kind of document that actually sort of lays out how it is different.

MS. SOTTO: Thank you for that comment. I think that is a very important point, and I think we

will take that under advisement and consider your comment in the drafting of the paper.

MR. TIEN: Okay.

MS. SOTTO: Okay, great.

Do we have any further comments over the phone?

Okay, thank you very much. Hearing none, we will move forward.

I will remind members of the public that you can submit written comments at any time by emailing them to privacycommittee@hq.dhs.gov. We will, certainly, respond.

Many thanks to our members of the committee who are present either in person or by phone. Thanks to our speakers and panelists. This was really an excellent meeting.

We are grateful to all for your interest in the work of the Privacy Office and the committee.

We will post minutes on the DHS Web site.

The URL is dhs.gov/privacy. The minutes will be posted in the near future.

With that, the meeting is adjourned.

[Whereupon, at 3:59 p.m., the meeting was
adjourned.]