U.S. Department of Homeland Security
Privacy Office

Data Privacy and Integrity Advisory Committee (DPIAC)
Public Meeting

December 10, 2018
90 K Street, N.E.
12th Floor, Room 1204
Washington, D.C. 20002

Transcribed by:
Alderson Court Reporting
Washington, D.C. 20036
(202) 289-2260

Table of Contents

Committee Members Present:

Lisa J. Sotto, Chair
Sandra L. Taylor, Designated Federal Official
James Adler
M. Peter Adler
Sharon A. Anolik
Jeffry Brueggeman
Dennis Dayman
Mary Dickerson
Laurie Ann Dzien
Joanna L. Grama
Robyn Greene
John Kropf
Sarah Morrow
Dr. Charles Palmer
Julie Park
Christopher Pierson
Tracy Ann Pulito-Michalek
Peter E. Sand
Russell Schrader
Dr. Robert H. Sloan
Chris Teitzel
C.M. Tokë Vandervoort
Marjorie S. Weinberger
Alexander M. White
Ron Whitworth
Richard Wichmann

Other Participants:
Ryan Baugh
James Burd
Debra Danisek
Sam Kaplan
Ashley Ortiz
Marilyn A. Powell
Marc Rosenblum
Jeremy Scott
Matthew Travis

PROCEEDINGS

Agenda Item: Roll Call and Opening Remarks

OPERATOR: Ms. Taylor, please go ahead.

MS. SANDRA TAYLOR: Thank you. We're ready, finally.

Good afternoon, everyone. Welcome to the public meeting of the Data Privacy and Integrity Advisory Committee. I'm Sandra Taylor, Sandy for short. I am the executive director of this committee.

We're going to start the meeting off by taking a roll call of all of our members. After that, I'm going to turn it over to Lisa Sotto, who is our chair. So remember when I call your name, just say "present" either in the room or on the phone, okay?

Jim Adler?

MR. JAMES ADLER: I'm here.

MS. SANDRA L. TAYLOR: Peter Adler?

MR. M. PETER ADLER: Present.

MS. SANDRA L. TAYLOR: Sharon Anolik?

MS. SHARON A. ANOLIK: Present.

MS. SANDRA L. TAYLOR: Suzanne Barber?

[No response.]

MS. SANDRA L. TAYLOR: Allen Brandt?

[No response.]

MS. SANDRA L. TAYLOR: Jeffry Brueggeman?

MR. JEFFRY BRUEGGEMAN: Present.

MS. SANDRA L. TAYLOR: Steve Chabinsky?

[No response.]

MS. SANDRA L. TAYLOR: Dennis Dayman?

MR. DENNIS DAYMAN: Present.

MS. SANDRA L. TAYLOR: Mary Dickerson?

MS. MARY DICKERSON: Present.

MS. SANDRA L. TAYLOR: Laurie Ann Dzien?

MS. LAURIE ANN DZIEN: Present.

MS. SANDRA L. TAYLOR: Melodi Gates is not with us today. She's not participating.

Lynn Goldstein?

[No response.]

MS. SANDRA L. TAYLOR: Joanna Grama?

MS. JOANNA L. GRAMA: Present.

MS. SANDRA L. TAYLOR: Robyn Greene?

MS. ROBYN GREENE: Present.

MS. SANDRA L. TAYLOR: John Kropf?

MR. JOHN KROPF: Present.

MS. SANDRA L. TAYLOR: Jeewon Kim Serrato?

[No response.]

MS. SANDRA L. TAYLOR: Sarah Morrow?

MS. SARAH MORROW: Present.

MS. SANDRA L. TAYLOR: Charles Palmer? Charles is on the line because I can see him on the line.

[Laughter.]

MS. SANDRA L. TAYLOR: Julie Park?

MS. JULIE PARK: Is present.

MS. SANDRA L. TAYLOR: Chris Pierson?

DR. CHRISTOPHER PIERSON: Present.

MS. SANDRA L. TAYLOR: Tracy Pulito-Michalek?

MS. TRACY ANN PULITO-MICHALEK: Present.

MS. SANDRA L. TAYLOR: Peter Sand?

MR. PETER E. SAND: Present.

MS. SANDRA L. TAYLOR: Russell Schrader?

MR. RUSSELL SCHRADER: Present.

MS. SANDRA L. TAYLOR: Robert Sloan?

DR. ROBERT H. SLOAN: Present.

MS. SANDRA L. TAYLOR: Lisa Sotto?

MS. LISA J. SOTTO: Present.

MS. SANDRA L. TAYLOR: Chris Teitzel?

MR. CHRIS TEITZEL: Present.

MS. SANDRA L. TAYLOR: Tokë Vandervoort?

MS. C.M. TOKË VANDERVOORT: Present.

MS. SANDRA L. TAYLOR: Marjorie Weinberger?

MS. MARJORIE WEINBERGER: Present.

MS. SANDRA L. TAYLOR: Alexander White?

MR. ALEXANDER M. WHITE: Present.

MS. SANDRA L. TAYLOR: Ron Whitworth?

MR. RON WHITWORTH: Present.

MS. SANDRA L. TAYLOR: Richard Wichmann?

MR. RICHARD WICHMANN: Present.

MS. SANDRA L. TAYLOR: Okay. And with that, we have a quorum, and we can start our meeting. So I'm going to turn it over to Lisa Sotto.

MS. LISA J. SOTTO: Thank you so much, Sandy. And Sandy, huge thanks for organizing us so well. We really appreciate it.

Welcome to committee members. We have some new members, and we thank you so much for your assistance -- and some longstanding members as well with us today.

Welcome also to our panelists and to members of the public who are here in person and some of whom are participating online.

For those viewing presentations remotely, there is a slight delay in the page turn. So please just be a little bit patient as the pages turn. To help us facilitate questions and comments from on the phone, as you saw, this is an operator-assisted teleconference. So instructions will be given as we open up the line for questions.

If you would like to ask questions, we're going to first take questions from the committee, and then we'll open it up. We'll have some time at the end of the day for questions and comments from the public. With respect to committee members, if you have questions or comments, I would ask you please to put your tent card up so that I can know to call on you. And if you could turn your cards my way so I could see your name? I know most of you, but not all of you. So I would appreciate that. So whenever you're ready with a comment, just do that.

And if you could please also -- we have a court reporter here. If you could please make sure that you say your name before you pose your question. Also, if you use acronyms, if you could please use the full name of the acronym because it's going to be hard otherwise to get it all down.

Logistics. Restrooms are out the door to your right, and there is also a vending area if you continue on down the hall.

We have a fantastic agenda today, and we're really just so delighted and honored to have the folks here who are going to be speaking to us, starting with you, Sam. So we will start with Sam Kaplan, Chief Privacy Officer and Chief Freedom of Information Officer, who is going to provide the committee with an update of the Privacy Office's activity since our last meeting, which was September of 2017.

We'll also receive a briefing on the new Cybersecurity and Infrastructure Security Agency. Currently, you all know it as the National Protection and Programs Directorate.

After that, we're going to hear from Marilyn Powell. Marilyn is the Privacy Office's Director of Incidents on the Department's breach response systems. Ashley Ortiz, in the U.S. Customs and Border Protection's Office of Field Operations, will provide an update on the Biometric Travel Security Initiative, after which our DPIAC head of the Policy Subcommittee, Chris Pierson, will present the full committee with our -- with the subcommittee's recommendations regarding privacy considerations in biometric facial recognition technology. The full committee will then discuss and vote on the recommendations of the subcommittee.

Following the recommendations vote, Marc Rosenblum, the Deputy Assistant Director in the Office of Immigration Statistics, will provide the committee with an update on Immigration Data Initiative. Joanna Grama, who is the chair of the DPIAC Technology Subcommittee -- DPIAC is the Data Privacy and Integrity Advisory Committee. Joanna will present to the full committee the recommendations of the subcommittee regarding privacy considerations in immigration data statistics. The full committee will then discuss those recommendations, and we will take a vote again on publication of the paper in final form.

We have reserved time at the end of the meeting for public comments, beginning at 3:45 p.m. If you are interested in addressing the committee, please sign up. You must sign up outside at the registration table if you are here live. For those of you on the phone, we will ask you if you'd like to address the committee, and we'll do that once everybody in the room has finished speaking. Please keep in mind that we may start the public comment period earlier if we get through our program, our full agenda more quickly than we expect.

I would ask that you all silence your cell phones and then we can get going with our program.

Sam, you are up first, and we are truly delighted to welcome you. We received a report last year, and now we have a new report that we'd love to hear about.

Thank you, Sam.

Agenda Item: Privacy Office Update

MR. SAM KAPLAN: Great. Thank you, Lisa. Thank you for your service in setting up the DPIAC for all these years. I know this is a big undertaking, and thanks to all the members for all the work that you've done to compile.

I do have some prepared remarks that will recap the year that we had, but before we get in, I want to thank Sandy Taylor for all the work that you've done in organizing this meeting here today -- and Sandra Debnam. Without the assistance of these two, the logistics of putting up a meeting like this wouldn't be worthwhile. Before we got started, I would be remiss if I didn't acknowledge their contribution.

MS. SANDRA L. TAYLOR: Thank you.

MR. SAM KAPLAN: So good afternoon, and welcome, everybody. I want to thank you all for taking the time to attend today's meeting, both in person and by phone. I'd also like to personally welcome the newly appointed members to the committee -- Dennis Dayman, John Kropf, Chris Teitzel, and Ron Whitworth. And thanks to all the DPIAC members and the subcommittee experts for the time and effort they've put into serving the Department over this last year.

As you can see from the agenda today that Lisa just recited, we do have a busy schedule planned for today. Rather than recap the day's agenda that Lisa just did, I'm just going to walk you through sort of the Privacy Office overview since the last committee meeting, which, again, was in September of 2017. As usual, there's been a lot going on in many areas of the Department, and I'm pleased and proud to give you guys a picture of how hard and how effectively our office has been working over this past year.

First, and most importantly, we issued a new Privacy Office strategic plan. On September 17th of 2018, I issued the Privacy Office's Strategic Plan for the Fiscal Years 2019-2022. You all should have received a copy, and it's also available on our website, www.dhs.gov/privacy.

The work of our office continues to support all the five core areas of the Department of Homeland Security mission. These are articulated in the Quadrennial Homeland Security Review, and that is prevent terrorism and enhance security; secure and manage our borders; enforce and administer the immigration laws; safeguard and secure cyberspace; and ensure resilience to disasters.

We also support the important cross-cutting goal that is articulated in the Quadrennial, and that is to mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities. Built around these six strategic goals, our Privacy Office strategic plan will drive the operations of the Privacy Office and help shape both privacy and the Freedom of Information Act improvements at the Department for the next 4 years.

First, with regard to staffing, some of our best professionals have moved on to other endeavors, but this creates room to hire new professionals and new staff and to continue adapting to the new needs as identified by the Department. First and foremost, Jordan Gottfried, our longtime Chief of Staff, recently, very recently left the Privacy Office just this month to join the Senior Executive Service in the DHS Office of the Inspector General, where he is going to be serving as the Deputy Assistant Inspector General for Management. We hope to fill his position. Though we know we will not be able -- it will not be easy to fill his shoes, we will have to fill his position.

Nicole Barksdale-Perry, our former Senior Director of FOIA Operations, she left in November to take on the role of Employment Services Manager in the DHS Office of the Chief Human Capital Officer. We are currently in a recruitment for this position. However, in the meantime, Jimmy Wolfrey is our current Acting Senior Director until a permanent replacement is found.

Christa Jones**,** who briefed the DPIAC committee at our last meeting, was serving as our Senior Director for Privacy Policy and Oversight. She departed last year to take a position at the Census Bureau. She is now serving as the Senior Adviser to the Acting Deputy Director and Chief Operating Officer at that bureau.

We also hired new staff this year, and I hope you'll all have a chance to meet these individuals and that they will all have a chance to work with the committee.

In February**,** Riley Dean joined the privacy compliance team as the Associate Director for Privacy Compliance. Riley was previously employed in the private sector.

In September, Amy Bennett joined our office on the FOIA team as a program analyst. Amy was previously employed in the Office of Government Information Services at National Archives and Records Administration.

In November, two new employees joined our office: Stephanie Boucher joined the policy and oversight team as a senior privacy analyst. Stephanie was previously employed at the U.S. Citizenship and Immigration Services. And Jaime Huang joined the compliance team as a privacy analyst. Jaime came to our office from a position at the Office of Management and Budget.

Additionally, this month we welcomed back David Lindner as the Senior Director for Privacy Policy and Oversight. David previously worked as a senior privacy analyst at the Cybersecurity and Infrastructure Security Agency's Privacy Office.

An additional major accomplishment this year is we established a Privacy and FOIA Council at the Department. Over the last year, we have been working at creating a community of practice for both privacy and FOIA professionals within

the Department of Homeland Security. In September, I signed the DHS Privacy Council charter, which created the DHS Privacy Council.

Concurrently, in November, and as the delegated Chief FOIA Officer for the Department, I signed the DHS FOIA Council charter, which created the DHS FOIA Council. The DHS FOIA and Privacy Councils created forums for sharing privacy and FOIA best practices; coordinating cross-cutting component challenges and developing solutions; and providing component privacy officers and FOIA officers a venue for raising emerging issues with our office and the senior management of the Privacy -- of PRIV.

With regard to outreach over the last year, as co-chair of the National Vetting Center Privacy, Civil Rights, and Civil Liberties Working Group, I brought a first outreach with the P/CRCL advocates on April 4, 2018, where our working group provided information on how DHS would implement NSPM-9, or National Security Presidential Memorandum-9. We discussed the NVC structure, as well as the interrelationships among NVC users, and the role of the P/CRCL Working Group and the National Vetting Governance Board.

Our partner organization, the Office of Civil Rights and Civil Liberties, organized a second outreach event with the advocates that was held on November 13th. At the November meeting, we were in a position to provide more details on the NVC structure and its governance, including a review and the public release of the P/CRCL charters and the governance for charters. And I'll talk in detail about the National Vetting Center in just a minute.

Additionally, we hosted other informational meetings with the privacy advocacy community to inform key privacy initiatives throughout the year, including topics of facial recognition and cybersecurity.

Some of you attended the July 10, 2018, meeting where members of the DPIAC's Subcommittee on Policy, along with officials from the DHS Privacy Office, CBP's Office of Privacy and Field Operations, toured biometric entry and exit operations at Orlando International Airport to observe general passenger processing operations, including the pilot entry and exit programs. Attendees at that meeting were briefed on data collection, usage, and sharing associated with the entry processing for arriving visitors, as well as a pilot program in which CBP has collaborated with British Airways to use biometric data -- facial images, specifically -- to verify a traveler's identity and process them for exit.

With regard to the Federal Privacy Council, again this year, the Privacy Office was instrumental in planning and executing the Federal Privacy Council's Annual Federal Privacy Summit on November 14, 2018. This is the only Government-sponsored annual event for Government privacy professionals. This year, Dr. Latanya Sweeney from Harvard University was the keynote speaker, and 32

privacy experts presented on 12 topics from blockchain to Government transparency to over 400 Federal privacy professionals and contractors.

With regard to fusion centers, in addition to ongoing privacy awareness training, both online and in the classroom, the DHS Privacy Office helped plan and participated in a privacy, civil rights, and civil liberties workshop for fusion center privacy officers and senior personnel that was held in Lincoln, Nebraska, on September 26th and 27th. Approximately 75 fusion center personnel attended, representing fusion centers from Guam to Florida to Vermont, and many locations in between. In August, Privacy Office staff provided introductory privacy training to 16 new fusion center directors and assistant directors.

Outside of these events, many of our staff provided privacy and FOIA training through numerous groups, including to privacy and FOIA/transparency professional organizations, and our component privacy colleagues did the same, expanding their outreach and making a deep and meaningful impact across the Government.

In addition to the normal business operations over the past 1 to 2 years, our office's attention has additionally been particularly focused on a few disclosure issues -- unprecedented number of requests for DHS records under the Freedom of Information Act, which have resulted in large, but manageable backlog numbers, and an increase in FOIA litigation.

Looking ahead, we expect to see continued growth in demand for our services. To meet this challenge, my office will continue to invest heavily in technology that allows us to seamlessly surge manpower against these backlogs, strengthen the Department's compliance with the Freedom of Information Act, and advance the use of best practices through the issuance of policy directives and instructions. And we will leverage services across the Department by using a cost-sharing model for FOIA processing and technology.

Working through the teams on the privacy side of our house, first the policy and oversight team continues to be active in meeting our statutory requirements to ensure DHS operations preserve and do not erode privacy. Mitigating privacy incidents remained a top priority for the Privacy Office, which we have also expanded our policy and oversight focus to include restructuring or reducing the use of Social Security numbers in Department mailings, as well as the privacy implications associated with the Department's implementation of National Security Presidential Memorandum-9, which is titled "Optimizing Use of Federal Government Information in Supporting the National Vetting Enterprise."

On the NVC, the National Vetting Center was created to better coordinate and enhance the vetting efforts of the U.S. Government for individuals seeking to immigrate to or transit the borders of the United States. The technical capabilities of the NVC will facilitate a collaborative interagency effort to more

efficiently identify individuals who may present a threat to national, border, homeland security, or public safety.

The NVC's operations will be governed by a National Vetting Governance Board, which established both a dedicated legal working group and a separate dedicated Privacy, Civil Rights, and Civil Liberties Working Group. I co-chair that P/CRCL Working Group, and it's chartered to ensure compliance with applicable law and to protect individuals' privacy, civil rights, and civil liberties.

PRIV, my office, has been engaged since day one of DHS's implementation of NSPM-9 -- influencing its oversight, its governance, and contributing significantly to its charter, the implementation plan, and other governing documents that will guide both its implementation and operation.

To facilitate greater transparency, the Privacy Office has advocated for the affirmative release of both the NVC and P/CRCL Working Group charters, as well as the NVC's implementation plan. The charters are posted on our public website under the FOIA Library, and we aim to post the implementation plan to that site once the FOIA review has been completed. Additionally, we plan to publish and post a privacy impact assessment of the NVC when operations begin.

The Social Security Number Instruction Policy, which was just implemented, outlines policy regarding the use of Social Security numbers at the Department of Homeland Security, and this instruction has been in place since 2007. This past year, however, in order to comply with the Social Security Number Fraud Prevention Act of 2017, which prohibits the inclusion of a full Social Security number in documents sent by mail unless expressly identified as necessary by the Secretary, PRIV launched a multi-phased effort to identify, inventory, analyze, and restructure the use of SSNs in mailed correspondence at the Department.

We have fully embraced the spirit of the act by conducting a holistic review of DHS's approach to SSN use to further reduce the collection, maintenance, and use of this sensitive personal identifier. While the Department's approach goes beyond what the act requires, it will aid the Department in reducing the unnecessary collection of SSNs. We are currently finalizing a policy that will require system owners to use an alternative personal identifier in place of the SSN or to mask or truncate the Social Security number whenever it appears.

If you haven't already seen it, we also published the first and second reports to Congress in July and November, respectively, as required by the act, which documents PRIV's multi-year plan to reduce the collection, use, and mailing of Social Security numbers at DHS.

With regard to incident prevention and mitigation, DHS's careful stewardship of the information entrusted to us is paramount to not only securing trust from the public but also securing the operational effectiveness of our programs. As we mitigate privacy incidents, new priority areas of focus may arise, which we are well positioned to take on.

You will hear more about our incident response a little later in our program from our Director of Incidents, Marilyn Powell. However, I should note that over the last year, the Privacy Office has crafted new and updated existing policies and instructions to comply with new OMB guidance and to facilitate incident prevention and mitigation.

In April, to raise awareness across the Department, we hosted, in conjunction with FEMA's National Exercise Division, the First Annual DHS Privacy Incident Tabletop Exercise here in Washington, D.C., with privacy representatives from all DHS components in attendance. The tabletop exercise examined, first, key DHS decisions required to address a privacy incident and, second, the roles and responsibilities as they are outlined in our Privacy Incident Handling Guidance.

This last year, the Privacy Office received additional funding in the FY 2018 Appropriations Act to ensure information and data released by the Department does not reveal the identity or personally identifiable information of non-U.S. persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. We worked closely with the Office for Civil Rights and Civil Liberties to develop a process to share information on incidents of unauthorized disclosures and to ensure that incidents are appropriately reviewed, investigated, addressed, and resolved.

The policy and oversight team continues to be active in a number of other high-profile areas, including ensuring privacy protections in the Department's collection and use of social media; our "big data" solution, or the DHS Data Framework; ongoing cybersecurity activities; and the development of an artificial intelligence in DHS operations.

On the compliance front, in Fiscal Year 2018, the Privacy Office adjudicated 72 privacy impact assessments. We put up 17 System of Records Notices. We adjudicated 1,151 privacy threshold analyses.

We now have a FISMA score of 98 percent for PIAs for all of our systems and a 100 percent score for all of our SORNs. These are the highest numbers in the Department's history.

Some of the notable documents published since our last meeting include three PIAs that describe facial recognition projects at the Department. The first is a proof-of-concept test by the Transportation Security Administration that

determined the viability of using facial recognition for identity verification at TSA screening checkpoints.

The second was a comprehensive CBP Traveler Verification System PIA. Many of you are familiar with the CBP's TVS efforts, and we'll hear about that today. CBP has spent several years testing various technologies in various locations to determine biometric technology that could be deployed in large scale without disrupting legitimate travel and trade, while still meeting the biometric exit mandate contained in the statute. CBP consolidated years of PIAs related to these tests to create a full privacy risk analysis to that program.

Most recently, the Privacy Office published the Secret Service Facial Recognition Pilot. This is a small-scale pilot involving volunteer employees. The Secret Service is testing the ability of facial recognition technology to identify known individuals and to determine if biometric technology can be incorporated into the continuously evolving security plan at the White House Complex.

We also recently published a PIA for the Science and Technology Directorate Counter Unmanned Aircraft Systems Program, which discusses measures taken to mitigate privacy risks and protect personally identifiable information during S&T's testing and evaluation of C-UAS technologies. This is the first PIA on this topic completed by the Government. The Science & Technology Directorate is leading DHS efforts and coordinating across the Federal Government testing and evaluating technologies used to detect, identify, and monitor small unmanned aircraft systems that may pose a threat to covered facilities and assets and other missions authorized by the Department in law.

Finally, we published a comprehensive PIA describing FEMA's Individual Assistance Program. This PIA was a large step forward in providing transparency for several systems FEMA uses to provide assistance to survivors of disasters.

With regard to the information-sharing, safeguarding, and security team, this is our third team, also known as IS3. This team consists primarily of senior staff who deal with some of the most complex, sensitive privacy work in the office, and they provide specialized expertise to the other teams on specific privacy implications of information sharing. This team supports a lot of the work of the compliance team by providing input and feedback on draft compliance documents based on their unique areas of expertise.

The IS3 team also represents the Privacy Office on a number of internal governance bodies, where our role has been written into the charter, and it helps negotiate Memorandums of Understanding that govern information sharing, so that Fair Information Practice Principles are incorporated into those arrangements.

The IS3 team also participates in the quarterly review of traveler targeting rules, which involves their review of the underlying intelligence that form the basis of those rules. We have an IS3 team member who happens to have both an aviation and background as a privacy expert and is uniquely qualified and certainly involved in all the guidance around the Government's usage of unmanned aircraft systems.

This team is also involved in international data sharing. I was in Brussels in October to attend the international privacy conference and to meet with world privacy regulators. They tend to be deeply impressed that we are able to be involved with and provide oversight of these types of sensitive activities. The European system, the data protection authorities are completely independent from their governments. This approach does have certain advantages, but it precludes many of them in certain instances from being involved with or even knowing about the sorts of sensitive activities being undertaken by their own governments.

While some of the work of the IS3 team cannot always be discussed publicly, it is exactly because of that team's work, our statutory structure of the Chief Privacy Officer position since DHS's establishment, which has been mirrored across several agencies and Departments, that we are able to embed privacy protections deeply into sensitive national security programs.

As you can see, we have been extremely busy over this past year. These are definitely exciting times to be a privacy professional at the Department of Homeland Security because we tackle some of the most complex privacy and national security issues that impact our society today.

Thank you again for taking the time to come and meet with us today, and I'm open to taking some questions from any of the members.

MS. LISA J. SOTTO: Thank you so much, Sam. Boy, have you been busy.

Happy to take questions, and I can start if the rest of you are shy. So I commend the Department's efforts on data minimization and the Social Security number state and certainly going beyond the statutory mandate. We have seen really a very significant effort now sort of across the globe and starting to talk seriously -- and it's been years in coming, but we're not very good at it -- to talk about data minimization and understanding that that's a critical piece of privacy and data security. Is there a wider effort across the Department to think about data minimization more generally?

MR. SAM KAPLAN: Well, as I'm sure you're familiar with, we utilize the DHS Fair Information Practice Principles, which minimization is --

COURT REPORTER: Can you pull the microphone closer? I'm sorry.

MR. SAM KAPLAN: All right. As I was just saying, across DHS, and this is -- I think it was in 2008 that the policy was implemented under the previous -- under Hugo Teufel, where we implemented the DHS Fair Information Practice Principles, and data minimization is part of that. If you look at our privacy impact assessments, we do a full FIPPS analysis for all of the programs that are conducted under a PIA.

And importantly, under the unique statutory authority of the Chief Privacy Officer, we do privacy impact assessments on programs and/or activities that would even fall outside of what is required by the E-Government Act. So, for example, when I was describing some of the facial recognition technology, the privacy impact assessments that we've done on the C-UAS technology, these are privacy impact assessments that only the Department would be conducting on programs and activities like that. Part of that, we look at the Fair Information Practice Principles, and minimization is something that we always look at, pursuant to those policies.

MS. LISA J. SOTTO: Thank you. Other questions?

[No response.]

MS. LISA J. SOTTO: All right. Thank you so much, Sam. We really appreciate it and really appreciate the great work that you and the Privacy Office are doing. Thank you.

MR. SAM KAPLAN: Thank you. Thank you, and I hope to get around to see all of you in person during one of our breaks. Thank you, Lisa.

MS. LISA J. SOTTO: All right. Let's welcome our next panel. On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act -- that's a mouthful -- of 2018. This truly was landmark legislation that elevated the mission of the former National Protection and Programs Directorate, NPPD, for those of you who are used to that acronym, both within DHS, and we established CISA.

The committee is very excited to hear about your work. Please help me to welcome Matthew Travis, Deputy Under Secretary, and James Burd, Acting Director of Privacy. Please proceed.

Agenda Item: The Cybersecurity and Infrastructure Security Agency

MR. MATTHEW TRAVIS: Thank you, Chairwoman Sotto. Appreciate it. Thank you to the committee.

It's great to be with you all. I'm here with my Acting Director for Privacy, James Burd, and it's a real treat to be here just 3 weeks into being a new operational entity.

So, as was stated, when the President signed the bill, it did a few things. One, it changed our name, which was welcomed, as NPPD was a bit grammatically clumsy and also a kind of amorphous, nondescript title that did not really speak to our mission. Having a name with "cyber" in the title is going to help with recruiting. It's going to help with the awareness with our stakeholders of exactly what our mission is and how we can help them. So that was a -- that was a plus.

The second thing it did is it is helping us to really focus the mission by, for lack of a term, spinning off two of our previous components, one of which you know very well, which is the Office of Biometric Identity Management, OBIM. The law calls for OBIM to transition to the DHS Management Directorate, and we're in the process of transitioning them. I think the final kind of conveyance will occur in early January. So OBIM, which had big, obviously, privacy equities and all the privacy officers that we were providing them, will go with them to Management.

And then the Federal Protective Service, again another critical mission, but it's a law enforcement mission, and I think the Congress saw that perhaps that was not something that needed to be in the Department's cyber agency. So the Federal Protective Service will go to a place that the Secretary determines. The law requires us to make a recommendation to the Secretary. There's a working group among us, FPS, and other parts of the Department to ascertain what the optimal disposition will be for the Federal Protective Service.

So what does that leave? So that leaves what really I think is the core and has always been the core of NPPD, now CISA, which is the cyber and physical security aspects of it. So when you talk about -- someone said, "Well, what does CISA do?" One, we're the leading cyber civilian -- civilian cyber agency in the United States Government. And we do -- we do, I'd say, five things.

We -- first and foremost, we defend the dot-gov domain. So through programs that you know very well, from EINSTEIN to CPF, to AIS, we work with all Federal agencies to ensure that their networks are resilient and help to respond when there's intrusions or attempts to do hacks. So that's one.

Two, in doing that, we conduct cybersecurity operations not just for the Federal Government, for State, local, tribal, and territorial partners, but also through the private sector, through the NCCIC, the National Cyber and Communications Integration Center. We deploy teams, the expert teams. We conduct exercises and training when they are again either left of intrusion or right of intrusion, helping stakeholders fortify their networks.

Thirdly, we conduct a number of capacity-building activities, both on the cyber and physical fronts through the National Infrastructure Protection Program, so those 16 sectors of critical infrastructure, working with the owners and operators to get -- make sure that not only their systems are resilient, but their actual machinery, their facilities, their people are all secure and protected. That's a very large part of what we do.

The fourth thing -- we've always done it, but the bill elevated it -- is emergency communications. Primarily, we help State and local governments with their interoperable communications during emergency response. We have a clock-spread element of emergency communications that I won't get into.

The fifth area that I'd say we do is national risk management. That's somewhat new and that would repurpose what previously was the Office of Cyber and Infrastructure Analysis, or OCIA. It's the National Risk Management Center. We did this in Lower Manhattan on July 31st with the Vice President and FBI Director and others in attendance. And this was really, I think, the biggest thematic change in the former NPPD, which is we need to work with private sector stakeholders much more closely. In today's environment, the nation-state threats are clear and present to critical infrastructure.

You know, when the Department was founded 15 years ago, it was primarily a department founded on the physical threats of terrorist groups. Fifteen years in, we see a very persistent and creative and daunting cyber threat from nation-states, as well as some transnational criminal organizations. So that imperative to defend networks, the Government can't do it alone. The private sector can't do it alone.

They need to see the threat intelligence more clearly and closely. We need to see, you know, their networks and understand what the architectures are to help better assist them and protecting them. So linking arms much more closely with the private sector, this notion of collective defense. "What's my risk is their risk, what's their risk is my risk" is really the push.

And so the National Risk Management Center, and I say it's not the National Risk Management Center -- it's the National Risk Management Center. We are looking to help those 16 sectors manage elements of what we consider national critical function. So when you think of those things that drive our economy, that enable our security, that really propel the American way of life. Things like elections, things like the electric grid, the clearing function in financial services, potentially the transshipment of iron ore through the Great Lakes, healthcare information and healthcare systems. We're actually in the process of working with those 16 sectors to determine what those national critical functions are, and in fact, they're meeting later this week, and so we'll be publishing that we believe those are.

And then, through the National Risk Management Center, bring in analysts from the private sector, but also from other Federal agencies -- Energy, the Pentagon, Treasury -- and start working the risk management campaign to not just share information. I think in the 15 years the Department did a lot to share information. We kind of pat ourselves on the back on how much information we shared. But we haven't actually taken it further to really work the problem collectively in the same room, looking at the same problem set, the same data, the same workforce, and understand what those vulnerabilities are, understand what the cross-sector implications and cascade impacts might be in the event of an attack.

And then, most importantly, work out what the mitigation plan is. So for any of those national critical functions, we are embarking on a campaign plan to help the owners and operators, as well as Federal agencies, better understand what those mitigation measures might be. They could be new laws and authorities. They could be new technologies, new partnerships and alliances, sanctions, what have you. But we can't just sit still while the threats to our critical infrastructure makes [audio disturbance] our actions that we take and [audio disturbance].

OPERATOR: Pardon me. This is the operator. There seems to be a lot of static on the line.

MR. MATTHEW TRAVIS: [Inaudible] components in the Department. Previously, we have attached [inaudible]. Now we're going to FEMA, ESA, nonconventional components, and we'll be standing up some of our own kind of operational elements. We've always had a Chief Privacy Officer [inaudible] the private sector, and some of you might know [inaudible] in the fall. We are needing that position. It's not because I think James is a great candidate. He is a great candidate. I've encouraged him to apply for it. But given the importance of privacy in CISA, we want to make sure we're conducting a nationwide opportunity to attract the best and brightest, and we're in the process of filling that position now.

[Inaudible] critical for a couple of reasons. One is that the nature of what it is we do is to [inaudible] and protect private PII and other critical information, right? So we think about cyber bad actors are either trying to do a few things. One, you know, vandals. That's not a concern as much. They'll work in the websites, deface them, what have you. More importantly is those who are trying to steal things, those who are trying to spy on us, and those who are trying to, you know, sabotage our infrastructure. All those three things are of great interest to us. And so we exist to try to help those 16 sectors, as well as State and local governments and Federal agencies, protect information. So if we think in privacy all the time, it's kind of why we exist.

Secondly, we have one regulatory authority, and that is the chemical industry. We regulate the chemical industry in terms of security efforts. Everything else is a voluntary partnership. All the capacity building, all the exercises and training,

all the assist visits, all our programs like AIS, those are all voluntary. And if large stakeholders don't believe that we're taking privacy seriously, that we don't have a very rigorous and tight operation when it comes to protecting our own information, being transparent about it, having proper oversight about it, then those partnerships won't work, and we will not be able to compel agencies, compel owners and operators to participate in these security-enhancing programs with us.

So James will talk a little bit more about the specifics of our privacy program. I'm happy to take questions at the end, but it's a real pleasure as the -- I'm still getting used to the name. I'm now the Deputy Director, instead of the Deputy Under Secretary. I think in Washington, if you lose words, that's a good thing. So I went from three words to two words. So I'm not complaining.

But let me introduce James, our Acting Director of Privacy, to continue on the description of CISA and privacy.

MR. JAMES BURD: Thank you for allowing me to speak today. Again, my name is James Burd.

COURT REPORTER: Can you pull that closer to you?

MR. JAMES BURD: My name is James Burd. I am the Acting Director of Privacy for CISA. It brings me a lot of personal pride to be not alone on just leading, but working within the Privacy Office for CISA. Not very often when you're a privacy professional do you actually enter a Government agency in which one of the inherent core missions of the agency is to protect privacy.

So, on one hand, I am looking at the issues associated with Government collection of public information and one-to-one private information. But on the other hand, to have that other piece of the pie in which the agency actually protects privacy is of utmost pride to myself and the members of my office. So I did want to give you a little bit of update on the ongoings at the Privacy Office at CISA today.

When fully staffed, our office is 11 members strong. But I do want to inform you that as the organization transitions, where the Office of Biometric Identity Management and the Federal Protective Service, they do have their own dedicated privacy staffs that were a part of my office. As they transition over, their talents will be leaving. That being said, the number 11 is what stands with the Privacy Office today without OBIM and FPS. We are looking at many measures to see whether we want to beef up the capability or not, but rest assured, our Privacy Office is fully capable and will be fully staffed.

I also want to make note that our office is a little bit unique when you think about other privacy offices in the sense that many privacy offices within the

Government serve as an administrative function or an oversight function. They will examine the work of their programs and components and integrate [inaudible] afterwards or help with the building of a system or a process beforehand. Our Privacy Office is operational. And what do I mean by "operational"? We do the administrative and the oversight stuff as well, but we also work hand-in-hand with the operators to actually go knee deep into the operations of the components.

So think of what I mean by that. Our privacy analysts are actually embedded into the operational activities of the organization. So not only are we responsible for the E-Government Act responsibilities or FISMA responsibilities, but we also have privacy analysts that work hand-in-hand with operators, discussing privacy issues, answering privacy questions. But also in real time, ensuring that our operators do not accidentally overcollect or ensuring that they do not go into areas which they are not supposed to.

It's a source of pride for our organization that privacy is operational, and that is something that it may not be a model for all organizations, and it definitely isn't a model for several types of organizations for a pure oversight role, but we are able to do so operationally, and I am proud to tell you about that.

And that's really all I have. I just wanted to give you a brief update on the office itself.

MR. MATTHEW TRAVIS: Thank you.

MS. LISA J. SOTTO: Questions from committee members? Mr. Pierson?

DR. CHRISTOPHER PIERSON: Thank you very much for that information.

COURT REPORTER: Can you pull the mike over, please? It's hard to hear you.

DR. CHRISTOPHER PIERSON: Thank you for that information today and the updates from November and the different changes that have happened within the operational component.

A quick question overall. In terms of, you know, been working on Federal workforce in terms of cybersecurity workforce, educating current workforce, filling positions of workforce, getting Congress to allocate new -- sponsor the workforce. So all the rations, probably about 2005 really this has been a constant theme. Are there any high-level observations and/or data points that you can give the committee on where it is headed, how well staffed it is, especially on the cyber mission, as this component moves forward in terms of what it's looking at in terms of the attraction and retention of cyber talent and all the rest?

MR. MATTHEW TRAVIS: Other than the threats from, you know, particular

nation-states, the biggest concern I have is our ability to attract and retain the human capital talent that we need to survive. We got a great competitive market for it, not only from the private sector, but the Pentagon and Cyber Command has a very large appetite for human capital, and so it's been a bit of a challenge.

We're behind on the numbers and where we need to be. There are some new programs. There's always the past couple of years been a cyber incentive, a retention program. But there's a whole new framework, the cyber -- CSTA, I think is the acronym. But essentially, it's a whole new way the Civil Service bringing in cyber talent that strips away some of the restrictions and limitations in terms of coming in and out of the Government, about what we can pay them, incentive pay, what have you.

So I'm hoping when that kicks in at the end of this calendar year, we can start hiring people under those authorities, that that will prove to be more effective than we've had. But it's probably the biggest push. I don't have any specific data points with me today on that other than it's a very high priority.

DR. CHRISTOPHER PIERSON: Do you know how many open seats you have that are in cyber positions approximately?

MR. MATTHEW TRAVIS: I didn't come prepared with those data here. I could get back and follow up with you on that.

DR. CHRISTOPHER PIERSON: Thank you

MS. LISA J. SOTTO: Mr. Dayman?

MR. DENNIS DAYMAN: Thank you, Mr. Travis, for your comments. I'm really excited to see what the future holds for you.

I'm interested to hear a little bit more about the private-public cooperation. I know there's things like I think there's about 80 or so of our member organizations around the U.S. What are the plans to sort of either continue to push those organizations to work with -- you know, for the FBI to work with local companies and that sort of thing? Are there other sort of interesting programs that you might be launching out of DHS that would help bring in those private companies to get more information, you know, whether it's from some of the centers and stuff?

MR. MATTHEW TRAVIS: Sure. So I think the biggest thing I would say is that I've noticed a change in the attitude from the private sector in that there is a unique and growing appetite for them to work with us, and I think this is because of the threat. I think this comes a lot from the banking industry. I mean Jamie Dimon, the JPMorgan Chase have been very vocal about the need for private sector to work more closely. And we see that also in the electricity sector. We

see it, and just, you know, look at what happened to Marriott last week.

And so I think the actual threat landscape is driving us -- driving them to want to work with us. And before either an aversion to sharing proprietary information or not trusting the Government is starting to -- those concerns are starting to wane.

The bigger program we have is the National Risk Management Center, again, which is a physical setting and which we're going to be bringing in analysts from the private sector. That's kind of a red tape-busting initiative in that in the Homeland Security Act, the Secretary has the authority to bring in private sector analysts. It's actually stated just like that. But we've always -- the Department has always gone through things like the loaned executive program, all these programs that take forever to get people in, whereas, well, it's like let's get a one-page MOU or MOA in place and bring your people in and sit down and get to work.

And so we're trying to really change the whole mindset of how the private sector works with us. We are now sponsoring SCIFs for certain members of critical infrastructure in which they have TS/SCI classified facilities so we can actually share more information. And it's those maybe not formal program -- the NRMC is a formal program, but trying to break through some of these restrictions and be more agile, more flexible, more forward-leaning, get them what they need.

MS. LISA J. SOTTO: Thank you. We'll just take two more because we're running way behind. Ms. Anolik?

MS. SHARON A. ANOLIK: Thank you. Thank you for sharing with us today.

The mission and scope of NPPD has changed now to CISA. How do you envision engaging with or leveraging this committee?

MR. MATTHEW TRAVIS: That’s an excellent question. I'll let James kind of tackle most of that. I think it's not that cyberspace continues to be, you know, not a brave new world necessarily, but it's a very dynamic environment in terms of the norms, the technologies, who's playing, who's doing what continues to change. I think we will need help and guidance -- and we certainly get it from Sam, but also from working with this committee -- to help understand what those left and right limits might want to look like. As we work more closely with the private sector, goes to show that we're becoming more collaborative with them and seeing which other networks we may be becoming more -- you know, in contact with their proprietary privacy information.

So I think I'm happy to come back every time you guys meet to kind of give you updates on where we are, but James, you're more the expert here. Do you want to talk about that?

MR. JAMES BURD: One item that I'd like to highlight as the Deputy Director's mission is the National Risk Management Center. If you have the opportunity to hear some of the advantages about the Risk Management Center or some of the activities that their leadership has engaged in, you'll have heard that there are sprints that we'll be undergoing for specific subject areas.

Part of the sprints involves not just a deep think within the Federal Government and the private sector entities, but engagement with other different types of organizations who have expertise in certain areas. One of the initial strengths that you may have heard about is the cyber supply chain initiative. This is where we are working with various members of the private sector, but not just them, but also areas that have done similar research in academia with regard to supply chain initiative.

Other areas that may be coming down the pipeline were -- sorry [inaudible] are position navigation and timing, PNT, or a lot of people know this as GPS. There is a task force looking at issues associated with GPS and the national redundancies and safeguarding of those systems. But as with any other task force or group [inaudible], they will seek private sector engagement, including those organizations [inaudible] that are not necessarily a private company.

So there are areas in which not only will we want to engage something like the DPIAC or other elements of civil society, but there is opportunities -- or there are opportunities for public outreach with these different programs.

MS. LISA J. SOTTO: And we would really be delighted to weigh in as you wish. We also have a subcommittee, the Cybersecurity Subcommittee, comprised of some members here and some members that are not on the full DPIAC who truly are experts in this space. So please use us as we might be useful to you.

Mr. Brueggeman?

MR. JEFFRY BRUEGGEMAN: Thank you. As one of the owners and operators that work with you, we really appreciate the collaborative efforts and the way that you work with the private sector.

Do you see any opportunities to expand, either convening discussions or leading any work with the private sector on privacy-related issues as a component of the coordination projects? It seems like that could be a helpful convening role that CISA could play on this issue.

MR. JAMES BURD: I will kick this one off. So I would like to point to a lot of initiatives that are put out by the Department of Commerce, particularly in this in the privacy risk management framework that they are working on. But there are also a lot of things that are going on with the NTIA as well.

More often than not, we do defer to Department of Commerce with those issues, but that's not to say that we would not be working with the private community with regards to cybersecurity.

MR. MATTHEW TRAVIS: Yeah, I think the convening power the Department has is very powerful in terms of being able to do just that without all of the formality that is sometimes needed through FACA groups, you know? Certainly amenable to it. Yeah, I think I need to work with James and team and certainly Sam to figure out what can we do more. You know, where is the demand signal and then how best can that be addressed?

MS. LISA J. SOTTO: Okay. We are deeply appreciative. Thank you so much for speaking with us.

MR. MATTHEW TRAVIS: Thank you very much.

MS. LISA J. SOTTO: And I will introduce Ms. Powell as she's getting seated. We're a little bit behind, and I apologize to everybody here. I'm going to cut your break just by a little bit, but let's plow forward.

Marilyn Powell, thank you for joining us. Marilyn is the Director of Incidents with the DHS Privacy Office. I understand it's your first time presenting before the committee, and we have provided various recommendations on breach response over time and look forward to hearing from you.

Thank you.

Agenda Item: Breach Response

MS. MARILYN POWELL: Good afternoon. I'm very happy to be here to discuss the Department's efforts to protect PII in response to a breach, but I'd first like to thank you for your February 2017 recommendations regarding best practices for notifying affected individuals of a large-scale data breach.

The Privacy Office executes victim notification in line with those recommendations. So that was a very valuable validation that we're on the right track.

I am the DHS Privacy Office Director of Incidents. I've been with the Department for 8 1/2 years. [Inaudible] of those years have been with the DHS Privacy Office, but only the past 9 months as the Director of Incidents.

The Director of Incidents position was created in 2017 because the CPO, or Chief Privacy Officer, recognized the need for a dedicated individual who could oversee the Department's privacy incident mitigation processes, ask our procurement process and system developers the tough questions, develop

policy, and cultivate Department-wide relationships to support the privacy incident reporting mitigation and remediation mission.

It has been an arduous road. That road has brought us to the strategies and the philosophies that we have today. Many of you have come along with us on that road, and we thank you for it.

I'd like to show the timeline. It starts in 2013. That's when we had our MSM Security Services incident. Also in 2013, we had our KeyPoint incident.

Then in 2015, the OPM breach. Of course, we found out later that the actual breach was in May 2014. So there we have contractor vulnerabilities one after the other.

And in 2015, the Department turned the corner with the [inaudible], and we began to institute our protection policies, such as the Homeland Security Acquisition Regulation costs in our contracts. We were looking to no longer have a one-sided matter when it comes to our data and contractor systems. PII safeguarding is spelled out in HSAR [inaudible], and we share the responsibility with the contractors from that point on.

COURT REPORTER: I'm sorry. Do you have the lavalier up high because it keeps hitting that thing? And keep your voice up. You're really drifting off. Thank you.

MS. MARILYN POWELL: How's that? Is that better?

COURT REPORTER: That's better.

MS. MARILYN POWELL: Thank you. We'll move right along into our June 2015 OMB Cyber Sprint, and from there, we instituted the Cybersecurity Implementation Plan, CSIP plan. So five objectives there, and it's more on the operational side, but I would like to show later that the DHS Privacy Office works alongside that strategy and in our own operational strategy.

In September 2015, Privacy asks the DPIAC for recommendations on victim notification. In July 2016, OMB A-130, Managing Information as a Strategic Resource, was instituted, and that's where our Chief Privacy Officers and senior agency officials for privacy, that's where they began to flex their muscle.

In December 2016, GSA instituted an Identity Protection Service, a blanket purchasing agreement so that in the event of a large, major incident, the Government and CISA would be prepared for the -- to have a credit monitoring in place and to service the victims quickly and efficiently.

In December of 2016, we also had our OMB A-108, which is the Federal

Agencies Responsibilities for Reviewing, Reporting, and Publishing under the Privacy Act.

January 2017 brought us to our modern breach response playbook. OMB M-17-12, Preparing For and Responding To a Breach of PII. Soon after, the DPIAC provided their recommendations for notifying affected individuals. And it was just in time, and it was very helpful for the Department to evaluate this process.

In May 2017, we had the DHS OIG breach. In December 2017, the Privacy Office instituted an instruction, the Privacy Incident Responsibilities and Breach Response Team. And there is where DHS Privacy Office began to flex its muscle and become more operational. We were able to put on our [inaudible] and brought that to the field and do our best for individuals that were affected by spills.

In December 2017, we posted our Privacy Incident Handling Guide, what we call the PIHG. In 2017, Equifax breach.

April 2018, the DHS First Annual Breach Response Table Top Exercise. May 2018, the DHS Security Office -- I'm sorry, Security Operations Center, what we call the SOC, joins our monthly incident practitioner calls, and there is where an integral and dynamic relationship is forged. We have the technical side meeting with the privacy pros and becoming more of a team, becoming transparent, teaching each other, communicating together on how we want to protect the data as well as protecting our systems.

And in September 2018, our very first Component-Specific Table Top. The entity now known as the CSIA was the first component to do -- to jump out the gate and to take on the responsibility and to take on the protections of the data that we collect and to look at how they institute their strategies. And it's been reported that soon USCIS, the collector and protector of a significant amount of PII, is looking into a specific -- component-specific table top in the first quarter of 2019.

So we're -- that was our arduous road that brings us to today, and what I'd like to show in this next slide is how the CSIP, with its five objectives on the strategy side -- I'm sorry, on the cyber side, works along with the privacy policy and oversight side. Our PII strategy parallels the five objectives of the CSIP.

Where on the cyber side, we're looking at continuous diagnostic monitoring, on the privacy side, we have a DHS incident Web portal we call the ECOP, and that allows us to continuously monitor our incidents Department wide.

On the CSIP side, when the objective is to identify high-value assets and to protect them, on the privacy policy and oversight side, we have our DHS compliance document oversight of those high-value assets.

When CSIP seeks to detect and respond, on the privacy side, we do the same. We are -- we instituted an instruction which allows us to operationalize our activities. The Privacy Incident Response and Breach Response Team, the CRT structure, as well as our PIHG, the Privacy Incident Handling Guidelines. It encourages our Department employees to recognize a PII spill and report.

When the CSIP seeks to recruit and train, we do the same on the privacy side. Based on the Executive Order 13719, the Federal privacy workforce, the Privacy Council was established in February 2016 that allowed us to launch a workforce effort in an attempt to attract and retain privacy pros.

And the last objective, acquisition and deploy technology. On the privacy side, we look at that as working with the procurement community and the contracting community to institute the HSAR clauses Department-wide.

Sorry. I'm having fun over here all by myself.

One of the most interesting truths that I've learned since joining the team is that there's really no memo or plan can solve our objective. Reporting is key. Frankly, what we don't know, we don't know. So successful messaging on reporting suspected and/or confirm privacy incidents must first be cleared, putting employees and contractors at ease. They have to feel comfortable to report known or suspected incidents with no fear of reprisal.

Reporting is our Federal Government sword, and the adage "Be careful of what you wish for" may well apply here. If you're successful in reaching employees and contractors, you're likely to also see an uptick in reported incidents, which means we need to be in the position to man the effort arising from potential incident reporting increases or report another issue and receiving information and reports on which we take no action.

So in a perfect world, we would like there to be no need, but realistically, however, daily headlines report one incident after another, and breach fatigue has set in through no fault of our own. As privacy pros, the DHS Privacy Office is challenged to continue to build on privacy [inaudible] practice, diligently pushing out best practices, partnering with component privacy officers to address circumstances where incidents are likely to occur, as well as recognize that if we can't prevent, we must have the rules to report, investigate, mitigate, and remediate.

The other thing I learned is that data stewards are everywhere, at every level of our mission. While attracting the privacy incident issue on all fronts is a must, that it has us involved in many of the Department's activities, such as partnering with the contracting community or partnering with civil rights and civil liberties to oversee special protected-class data handling. Or providing training and scripts to our IT customer service phone reps. DHS privacy is everywhere because the

data we collect is everywhere.

So that arduous road that we went down together brings us to today. Our strategy is pretty simple, really. We never forget who owns the data. We strive to service and protect the victim. We implement preventive measures. We have monthly incident practitioner calls. Those calls get pretty lively. Everybody is engaged and interested and committed.

We'll continue having our DHS Annual Breach Response Table Top Exercises. We will continue to seek advice from the DPIAC. And of course, we will continuously monitor and [inaudible] visibility into our known and suspected incidents Department wide.

But our overall goal is to remain flexible because no privacy incident is exactly the same. We continue to call on the Department to remain fluid and responsive, and because neither the cyber nor the privacy policy side can afford to become jaded or entrenched in the old response strategies, we must stay agile and remain flexible. It's amazing how many new and creative ways we have to control data. But we just have to be committed to spring into action when it happens.

So I thank you for giving me the opportunity to speak to you and to share with you what has brought us here today and to have the opportunity to let you know that the Department is committed to protecting the data that we collect.

MS. LISA J. SOTTO: Thank you so much, Ms. Powell. You see a lot of sympathetic faces around the table here.

[Laughter.]

MS. LISA J. SOTTO: You know, we -- this is one area where I think we in the private sector have a lot to share and lessons to share with you. So please do invoke our services as needed. We have been doing this for a long time in the private sector. So I would dare say we are better than anyone in the world on the private sector side in the United States because the first breach notification law went into effect on July 1 of 2003. So we've been doing this for a while.

I just have one very quick question. What is the official timing for notifying affected individuals when after a discovery of a data breach?

MS. MARILYN POWELL: There’s no official timeframe. Really, it's on a case-by-case basis. First, of course, the risk of harm, but there are other factors involved. If there are law enforcement issues involved, our Breach Response Team will weigh when its best to -- and you don't want to notify too quickly before you have all the information, before you have all the details. That doesn't -- that only serves to create hysteria, as opposed to giving -- to giving your victims

information. So it's on a case-by-case basis.

MS. LISA J. SOTTO: Thank you. Questions?

MR. RICHARD WICHMANN: Ms. Powell, how --

MS. LISA J. SOTTO: Could you just say your name, too?

MR. RICHARD WICHMANN: Okay.

MS. LISA J. SOTTO: Please remember, you guys, to say your name prior to questions.

MR. RICHARD WICHMANN: Ms. Powell, my name is Richard Wichmann. I wanted to know how you are looking at third parties as far as potential incidents. To the extent there are third parties involved with DHS and have access to information, how are they rolling into your incidents? How do you -- if there is a breach there, how does that come into the program?

MS. MARILYN POWELL: When the third party has control of our data?

MR. RICHARD WICHMANN: If --

MS. MARILYN POWELL: Well, we are very aggressive about contacting that third party and walking every step along the way with them. And when we get our incident practitioners together, we find out how many components are actually affected by the third-party breach, and those particular components work together. We share information. We go out in different directions in order to get -- to gather in the facts, and you apply as much pressure as you can to making sure that the third-party notifies all of the affected individuals, perhaps even allows our security operations center, our IT team to go in and view or get a visual on what's going on.

So we -- a third-party incident is a little less work for us, but not really. We take it as if it's our data. So it's not our breach, but it's our concern from the moment we know about it.

MR. RICHARD WICHMANN: Thank you.

MS. LISA J. SOTTO: All right. One last very quick question.

DR. ROBERT H. SLOAN: Microphone? I'm truly loud. Robert Sloan. Speaking of third parties, I was wondering with all of these Government incidents why the Equifax breach was on your timeline of Government incidents?

MS. MARILYN POWELL: Because Equifax is a partner with the Department,

and they do background checks for our employees. And so we were -- we were touched in that way. And we went through the same steps with Equifax as we would with any other third-party vendor.

DR. ROBERT H. SLOAN: Thank you.

MS. LISA J. SOTTO: All right. Thank you so much. We very much appreciate your speaking to the committee. Thank you.

MS. MARILYN POWELL: Thank you.

MS. LISA J. SOTTO: Let's take 5 minutes. If we could be back here at 2:37 p.m., that would be great.

Thank you very much.

[Recessed at 2:32 p.m.]
[Reconvened at 2:44 p.m.]

MS. SANDRA L. TAYLOR: Hi, everyone. We're going to get started.

[Pause.]

MS. LISA J. SOTTO: Terrific. Welcome back, and a quick reminder to please silence your cell phones and another quick reminder that we are taking sign-ups for public comments right outside the room, and we'll start that at 3:45 p.m. We certainly will not be getting to it early, given how we're doing today. We're pushing the envelope on time.

But please do sign up if you have -- if you're a member of the public and you'd like to comment or ask questions of the committee.

Our next panel is going to provide an update from U.S. Customs and Border Protection on the Biometric Travel Security Initiative. Please welcome Ashley Ortiz, management and program analyst, Entry/Exit Transformation Office, Office of Field Operations.

Welcome, Ashley.

Agenda Item: Biometric Travel Security Initiative Update

MS. ASHLEY ORTIZ: Hi, welcome. I think I'll hand it over to Debra Danisek, who is our privacy officer for CBP, and we work really closely with her.

MS. DEBRA DANISEK: Thank you, Ashley. Is this on? Yes-ish. Okay.

So not to steal Ashley's thunder, but I just wanted to thank the committee for having U.S. Customs and Border Protection speak today. As I'm sure you can imagine, we are one of the quieter components within DHS, never anything going on at CBP. Just very, very, you know, go with the flow.

But I also wanted to thank many of you who I recognize from our trip to Orlando a couple of months ago. Ashley is going to give a great overview of our program, but we were really delighted to be able to show this program in person to several of the committee members and look forward to more hands-on trips like that in the future.

So, again, my name is Debra Danisek. I'm the CBP Privacy Officer. My email is in the back of Ashley's presentation and happy to -- happy to discuss any of this with you guys following the presentation. So go ahead.

MS. ASHLEY ORTIZ: All right. We'll go ahead and get started and try to be mindful of the time. I also have a few other CBP colleagues sitting behind me that might chime in during the presentation or with questions. It's really a group effort here.

So, first, we'll touch a little bit upon the long and at times challenged history that CBP and really the Department of Homeland Security has faced in implementing this congressionally mandated biometric entry and exit system, starting in the early 2000s. And since then, DHS and, beginning in 2013, CBP have implemented various pilots, which has provided us with some key information that helped us get to the solution that we developed today.

So really what we learned throughout these pilots is that, one, stakeholder participation is critical in really achieving our vision for enhanced security, but at the same time, facilitated travel. And second, that we didn't want to add any additional process to the current procedure. We really wanted to use the current infrastructure that was already in place.

And so what that helped us accomplish is our current vision, which is a facial matching service that leverages existing advance passenger information data that the airlines already provide us, and using that data, we pull photographs that are already in our holding. So this would be photos from previous CBP encounters, the U.S. passport database, U.S. visa, and what we do is build a flight gallery because, again, as I mentioned, we already know who's going to be on that flight.

So as this individual boards the flight, they would -- or on entry as well, you would take a live photo, and that live photo would match one of the photos that's already included in the gallery. And so, at that point, we would create an exit record, and that individual would be biometrically confirmed for those that are in scope for biometric exit.

So the reason why this solution works really well, and it kind of goes back again to those two main points that we learned throughout the various pilots, is that we're able to work with our stakeholders. This is something that in the air environment, we're doing with the airport and the airlines, already using it in their current travel process. So as they board -- and I'll show you some pictures of that in the next couple slides. As they board, they're able to take a photo, and it's not adding anything new. We're also using an existing biometrics. So we don't have to add an enrollment to it.

So, for example, the U.S. Government does not have much information on iris. So if that was the biometric modality that we would use, that would require some sort of enrollment process, which would really make the process a bit more complicated.

And so this system is also able to be used in the land and the sea environment, and what we're really doing here is replacing a manual process with an automatic one. So it limits the number of times that you're showing your ID or your passport to someone within the travel continuum, which, as I'm sure you all know, it starts at check-in and it continues throughout until you actually leave the airport.

So a quick slide of how this actually works upon entry and exit. And what we're really calling it is a simplified travel vision because that is part of our vision, to enhance the travel continuum and make it as seamless as possible. So, upon entry, again, you would use this same process. We know who's going to be on the flight. We know who's going to enter the United States. So we build a gallery, and we match your face, your live photo to the gallery of photos that we already have at hand, which simplifies that entry process and allows our officer to really focus on the interview aspect.

And again, on departure, we would be able to use your face. Again, take a photo instead of having to take out your ID over and over again. So at the same time, we enhance security, but we facilitate travel and really make it something easy for the traveler to do.

So, again, as I mentioned, simplified arrival, what we're doing in air is using your photo to enhance the process, allowing our officers to really focus on what they're trained to do. You know, part of the interview, more interaction with the traveler and less of the swiping the passport, you know, taking the fingerprints, letting them get back to the nature of their work and really focusing on that admissibility interview.

And we've already caught three imposters at Dulles airport. I'm sure you guys have seen some of the press releases. If not, we're happy to share those about the three imposters that we've caught using this system. So it really has that

security element there. Currently, we're at 15 locations, including 4 preclearance locations.

In terms of simplified departure, what we have here, and again, one of the great things about this system is that we're really working with our stakeholders. Our system is device agnostic, meaning that the stakeholder can decide what front-end equipment they would like to use while CBP manages the back end. So you'll see here, there's a JetBlue model very similar to a camera on a stick that JetBlue and others -- for example, at Dulles and Reagan, they're also using kind of like an iPad on a stick model.

Others, in Los Angeles and in Orlando are using more of a gate model. So we're really letting them decide what works best for them, but the same sort of back end. And in the instance where there is a no match, they would just go back to manual processing. So really no -- no negative for the traveler. This is something that they are familiar with. They would step out of line. The airline agent would just look at their travel documents, and then on they would go.

And so, in 2019 and the years to come, we really do have an expansion plan to work with our stakeholders, and these names have been released publicly, which is why we can share them today about where we're thinking about going with these stakeholders hand-in-hand in the future.

Some of the benefits that we have seen, for example, on entry is that we're able to clear the flight a lot faster than we were in the past, which is a major benefit not only to our officers, but also to the airport and our stakeholders as well, as I mentioned, a better use of our staffing. The officers are now able to get back to that admissibility and enforcement focus instead of that more administrative work.

And then in terms of boarding, our stakeholders have reported boarding 350 passengers in about 20 minutes or so, which is it's a great increase -- or decrease of boarding time for them, as well as being able to meter passengers better. So I think one of the worst places to be waiting is on the jetway to get to your seat. So you're all excited after you pass the boarding gate, and you know, you see the agent, and you're like, okay, I'm ready to go. And then you wait some more. So this has really helped meter those passengers there.

So in terms of just our operational performance, CBP does, in conjunction with our partners at Science & Technology and our partners at NIST, we do a lot of rigorous testing to review our data and metrics, and we, you know, actively monitor and refine our performance. And so, in total, we've seen over -- we've processed over 5 million travelers using this entry/exit system.

So outside of the entry/exit realm, we're also partnering with TSA, which is a force multiplier for us. And so, as you know, again, part of the always pull out

your ID process, with TSA, there is yet another agent there that's looking at your identification and checking your ticket as well. What we're trying to do there is replace that with facial recognition.

And so not only does that, again, enhance security, it facilitates travel. But it's also reassuring to our travelers and our stakeholders because you have two Government agencies that work in similar space, and oftentimes, they don't use the same process or the same systems. And you've got kind of two processes that the traveler and the stakeholder have to go to. Working with TSA, with our brothers at TSA, we're able to implement one process, which makes it a lot easier for all of our users.

As I mentioned before, the system also transfers into the sea and land arena. With sea, we're doing a very similar layout, as we are with land in terms of partnering with the industry. So we have a few sea pilots going on now, and early results indicate again a lot of that enhanced enforcement activities for CBP and really facilitating travel.

In land, I think this is something fairly new, especially for the members that were able to tour in July. We have launched our land pilots, so vehicle at speed in the vehicle environment. And what we're doing is capturing both inbound and outbound travelers in vehicles, not only the driver and the passenger, but really two and three rows back with a fair amount of accuracy, although that is in the pilot phase.

And again, in pedestrian, we have launched an entry in both San Luis and Nogales, and especially on a security front, we have already caught 45 imposters, actually. I double-checked this morning. I made this PowerPoint last week, and last week, it was 38, and now we're at 45. So we could definitely see that that is a big enhancement.

One thing that I did want to mention in the land environment that I think it's something that the members wrote about in their recommendation is about the signage. And definitely in the land environment, we have taken that into consideration, and you'll have -- you'll see signs in both English and Spanish, given the traveler population there.

So I will turn it over to Debra to talk a little bit more about privacy.

MS. DEBRA DANISEK: Sure. So I think it’s very fitting my colleague James Burd, who spoke before me, mentioned operational privacy and how lots of the Government privacy offices are, you know, administrative, and then maybe oversight. Well, with this program, I mean, this program has really gone above and beyond to work with my staff, and they have their own privacy support as well to operationalize their commitment to privacy.

So we have done a considerable amount of outreach. We've done listening sessions for privacy advocates here in the Washington, D.C., area and then also in San Francisco. We have briefed the DPIAC several times, and like I mentioned, we were happy to host some of you to go and see the technology in person in Orlando.

And we have been anticipating the release of your report and recommendations. We are always looking for ways to do this better, and so we certainly appreciate the recommendations that the DPIAC has provided and also the feedback that we get from either members of the public or the privacy advocacy community. We take all of that into account to try and figure out how to build this better and meet our mission needs.

This program has also been prolific with the privacy impact assessments, if you haven't read them all. There are over 10. We've recently republished them into one sort of comprehensive privacy impact assessment called the Traveler Verification Service, which published on November 14th. That's a comprehensive risk assessment, privacy risk assessment of this entire program and really gets into the details on the Fair Information Practice Principles and how we have implemented this program in a privacy-protective manner.

There's also quite a bit of content on CBP.gov. As the DPIAC members saw in Orlando, we do a time of collection, point of collection notice for the travelers as well so that they know that this is a CBP information collection. Typically, the gate agents will read sort of a notice, or it flashes on the video screen that says, you know, this is the flight to wherever. There's also a big sort of Government-looking sign that's posted right there at the boarding gate that the airport authority can move around if the technology is used at different -- different gates.

And then, of course, U.S. citizens who don't wish to participate, U.S. citizens or LPRs can opt out. They just have to tell the person taking the photo that they don't wish to participate, and they just go see a gate agent and can proceed as normal. That's also what happens -- I get a lot of questions on, well, what happens if there's no match or if it doesn't work? Isn't that embarrassing for the traveler, or you know, what's the impact to the traveler if they don't match while they're standing there?

And there really is no impact. They just go right to the gate agent, and they do a manual check of their identity documentation, and it does happen to a handful of folks each flight, for whatever reason, and there is no -- there is no sort of embarrassment or -- or issue with someone either opting out or going to see the gate agent.

So on the next slide, very small up on the screen, but that's okay. So we talk about privacy by design and CBP OFO's, Office of Field Operations' commitment to privacy. So there is a change, actually. So I said we are always looking for

ways to do this better and be more privacy protective. I understand that it's a new technology. This is a major shift in how you board an airplane.

So in the DPIAC report and in previously published privacy impact assessments, we did say that we held U.S. citizen photos for 14 days. But we have made the technical change based on feedback from -- from the DPIAC, from the privacy advocacy community, and because in keeping with the data minimization theme that we were talking about earlier, since we don't enroll U.S. citizen photos, we don't really need them once the match is completed. So they are -- they are deleted from the gallery after -- from the matching service after 12 hours or no later than 12 hours. Typically, it's right after the flight departs.

So that keeps with our data minimization and use limitation principles that we are literally just verifying that you are the person that should be getting on this airplane if you're a U.S. citizen or lawful permanent resident, and then we delete the photos.

For in-scope travelers that are non-U.S. citizens or non-lawful permanent residents, then we do create an enrollment in our DHS IDENT system, which is the biometric repository, and we have partnered very closely with the airline and airport partners to ensure that their business requirements do not allow them to retain the photos either. So we do that through contract provisions and the business requirements for the airport authority to deploy this technology.

In terms of security measures, this is all laid out in detail in the privacy impact assessment, but there are very strong security measures like encryption, access control, and the templatizing of the photos so that they're irreversible and can't be -- cannot be hacked from the matching service. And then there's always -- I mean, obviously, there is concern with facial recognition technologies with the bias of the algorithms. And so this is a rapidly evolving space, technology space.

I actually saw a very interesting report that came out from NIST a couple of days ago, maybe it was yesterday, that said there had been an industrial revolution in the area of facial recognition and that the new algorithms even from 3, 5 years ago are far superior to those algorithms from 3 to 5 years ago, and so the match rates are much, much higher.

We are actually partnering with NIST to help develop and ensure that we are using the highest-quality algorithms available to do the matching, and so it's very encouraging that NIST has taken this on as a project, and we continue to partner with them. Like I said, we are committed to doing this right and in a privacy-protective manner. So whatever assistance they can provide or industry or the advocacy community, you know, we're open -- we're open to hearing it.

So, so I don't know, did you have anything else to add?

MS. ASHLEY ORTIZ: No.

MS. DEBRA DANISEK: No? Okay. So that's our contact information up there, and like I said, we really are open and transparent about this program. It's probably the most transparent program that we have at CBP in terms of all the efforts that the team puts into the privacy compliance work. And so happy to take any questions, and we're happy to brief you guys anytime.

Thank you.

MS. LISA J. SOTTO: Thank you so much, and we may -- we would love to hear how you're doing over time. Let's just keep questions to a real minimum. We'll take Ms. Greene's question, and then we're going to roll right into the subcommittee's report.

MS. ROBYN GREENE: Okay. I don't know if supposed to have a microphone?

MS. LISA J. SOTTO: Yes, you are.

MS. ROBYN GREENE: So I'll be very brief. I just have one brief comment and then a couple questions, which you can answer now or come back to us on since we are under such a time crunch.

My comment is just with regard to the possibility that there are a handful of people on each flight who do get sometimes correct, but sometimes false mismatches. I think that there should be consideration given to the idea that they may be embarrassed by that.

Oftentimes, people who have lower -- or higher false positive or false negative rates are people who are members of communities that are subject to more surveillance, who are subject to more policing, and oftentimes in the travel context are subject to additional screening by TSA and other folks. And so these are people who may feel embarrassed if they're pulled aside and have to go through a different additional screening or an additional process. They may also suffer a delay or a missed flight.

And so, and that sort of leads me to one of my questions, which is, is there always going to be someone at the gate on hand to do that manual review so that there is no additional delay? And in the future, once there is sort of full deployment, it sort of seems like the [inaudible] would be to have less humans actually doing this kind of work, and so how will you be accounting for that?

Another question I have is about efficacy. It's great that you're identifying imposters, but I think relevant information is not only how many imposters are you identifying, but how many people are you identifying under manual conditions, and what's the comparison there? Any time you're collecting

additional data, you are creating an additional opportunity for a data breach. And so I think the measurement for success is not only does this identify imposters, but does it identify imposters at a rate that is greater than that which a manual one would, and that added risk is accounted for in the increased efficacy.

And then my last question is just I would love some more information about how you are planning to deal with decreased rates of efficacy at land borders, when you're not only drawing from small sample sizes like you might be from a flight manifest, since the more -- the larger your sample size for facial recognition technology, generally the lower your accuracy rate.

MS. DEBRA DANISEK: Those are great questions. There's a lot there. So --

MS. ROBYN GREENE: Sorry.

MS. DEBRA DANISEK: Nope, there's a lot there. So I will say, so to the first question, we partner very closely with the Office of Civil Rights and Civil Liberties at DHS. We gave them a tour of the technology and a demonstration at Dulles about a month ago.

But to your point about embarrassment, I think that's a popular question, actually, that comes up in the advocacy community quite a bit, and I think that I would almost rephrase it. Because I -- having seen a lot of this in person, it recognized someone with a hijab and glasses on, for example. That was a match.

But someone who is in a wheelchair who the camera couldn't reach because it was stationary, then they had to get the gate agent to come and for manual verification of that person's identification. So, so I think it can vary on what sort of person may not be able to use the technology or be a mismatch.

That said, yes, there will always be a person there to do the physical, the check, and it's usually the same person that's taking -- standing there next to the camera to tell people where to look. So the couple of seconds that it might take to say, "Oh, you know, please let me see your documentation," there is no getting out of line or what not. It's the same person that's taking the photograph there. Usually they're helping with sort of the flow of the line as well;.

So, but that's an excellent question and something that I think we are very aware of, you know, when we deploy it and want to make sure that we're cognizant of those sorts of issues. Children are another one that they often don't match either. So -- so, you know, you have to have a gate person or an agent there as well.

To your efficacy question, which is also a good one, so unfortunately, those are not metrics that we could provide, right? Because if we were to say publicly the percentage of imposters that an officer manually missed, then that would be a

very large operational security issue to the frontline agents because then you would know, okay, well, X percent of the time, if I'm -- you know, a human could not make this sort of identification.

So those are numbers that we have and that we monitor, but it's not something that we're comfortable, you know, putting out as a reason why this is successful. I do think that these success stories about the imposters that we are able to catch, you know, those are not -- those are folks that we wouldn't have caught before. So it's showing that the technology does -- does work, and it's a success story.

And what was the third question?

MS. ASHLEY ORTIZ: The third question was about the gallery size at the land border. I think that's something that we're currently looking at right now. That pedestrian pilot has been in place since October, and so really what we're doing now is trying to see what is the right gallery size. We are very cognizant and aware, just like you said, it's not like the air environment.

So we do see that, and we're working very closely with our partners at Science & Technology. We're going to begin working with NIST soon to address that kind of with the field experts.

MS. ROBYN GREENE: I think it would be helpful to have more information for us about where you'll draw the data from to populate your gallery. Because you know, it's very clear in the like air travel context where you get those data, right? If you're traveling internationally, you have passports. But if you're, you know, just taking a day trip to Mexico City or to Montreal, that's a very different kind of story --

MS. ASHLEY ORTIZ: Correct.

MS. ROBYN GREENE: -- and it's not like we're notifying folks.

MS. ASHLEY ORTIZ: My colleague reminded me right now we're doing one-to-one. So it's not that gallery size, but you'll see in the privacy impact assessment that a possibility is to look at frequent border crossers. Now, again, we are looking at what does that mean? Is it every 30 days? Is it someone who crosses every day or every 6 months, or what does that mean? So we're not -- we understand that, and I'm happy to brief you all once we get to a point where we think, yes, this is an appropriate gallery size. But we're not there just yet.

MS. LISA J. SOTTO: All right. I'm going to turn to Ms. Park to ask a few questions. If you could please just take them back and respond to us later? And I apologize for that. We're just running very tight on time.

MS. JULIE PARK: Okay. This is -- my name is Julie Park, and my questions for you are in the tasking that you provided to the committee, it did not include in the tasking questions about choice or opting in of biometric scanning, and I was just wondering why that was not included in your request as per the task?

And then the second question I have is I'd just like to know, as part of the privacy by design, under FIPPS, you have the use limitation and purpose specification. How does that apply to both live photos and specifically existing photographs? So when you're gathering that through passports, how are you applying the use information and purpose specification?

MS. LISA J. SOTTO: And I think with respect to the tasking, that's a tasking actually from the Privacy Office. Am I correct about that? Yes. And so that would be an appropriate question for the Privacy Office.

Okay, good. All right. Let's move on now to Dr. Pierson, who chairs the Policy Subcommittee of the DPIAC. Chris is going to present to the full committee the findings regarding privacy considerations in biometric facial recognition technology, and then we will ask the full committee to discuss and then vote on the recommendations.

Mr. Pierson -- Dr. Pierson?

Agenda Item: Subcommittee Report -- Biometric Facial Recognition

DR. CHRISTOPHER PIERSON: And just noting for the record, Rick Wichmann excusing himself because of a conflict. Perfect. Thank you, sir.

All right. Can everyone hear me? Everyone awake? Everyone back there awake? Yes, good. All right. Well, got a few votes. Good.

So thank you very much, Chief Privacy Officer Kaplan, Deputy CPO Jonathan Cantor, as well as special thanks to Sandy Taylor, Sandra Debnam somewhere for all of your -- there you go -- all of your help, as well as to the Policy Committee. This has been about a year that we've been looking at this, a lot of good effort, a lot of good comments, and a lot of meetings around this topic of biometrics and facial recognition.

Also thanks to the folks from the public as well as Government sector that are here with us today.

DHS has an incredibly important role here in terms of preventing terrorism, especially in the role through CBP at our borders. We were issued a tasking from the Privacy Office in September of 2017. This tasking was very finite in

terms of the different things that it wanted us to look at.

The DPIAC is, in effect, an advice and guidance -- serves an advise and guidance function into the Privacy Office for DHS, and we're responding to those different items that we have been tasked with. Over that yearlong journey, we've done several things. We held a public hearing back in September of 2017 where CBP went ahead and briefed the entire committee on its program of biometric facial recognition. We also met separately, the Policy Committee separately met with CBP in May of 2017 -- or 2018 for further questions, diving deeper into the different items that we were interested in.

We also met with the academic community. So specifically, Georgetown, their technology center, policy center, Laura Moy's group. We spent a lot of time with them. At the end of 2017, there was a paper that was released about facial recognition, especially in its use for securing the air travel industry and airlines. And so we met extensively with that team, the entire Policy Committee, and asked them a lot of different questions, heard some of their thoughts, their comments, their concerns. We were able to bring some of those back to CBP and go through them.

This was actually a really unique exercise that Debra really alluded to it a little bit. We went onsite. So four of us traveled to Orlando, Florida, where we went onsite, actually examining all aspects of the entry program, the exit program, specifically British Airlines -- Airways terminal and the onboarding process. We stood there and watched the entire process, the notices. We looked at the travel immigration entry in terms of the notices and consent, peering over the shoulders, if you will, of the different CBP officers and agents, really connecting the policy, the legal, the warnings and notices with what was operationally told to us what was happening both in September and May of last year.

Some comments from the public community, as well as watching and looking at what we saw with our own two eyes. And did we hear the notices being spoken over the loudspeaker? Did we see folks making their way through the actual gates? I have to say that informed us deeply on our different opinions on some of the conclusions that have been made.

Let me go ahead, and I know that time is kind of waning here. We want to make sure we have good time for public comments. First, we looked at four real trickle areas. We looked at areas and topics of notice, topics around facial matching algorithms, really data quality and integrity. We looked at partners and data protection there, as well as usefulness in terms of time of photographs and facial recognition being used in accordance with that.

In terms of notice, you know, literally, we found exactly what was described to us -- oral notices, written notices, notices with sufficient time period, be able to read them. There were some observations there in terms of furthering the quest for

readability, making sure folks had access to electronic devices when links were referenced, when websites were referenced, and also noting the complexities of land crossings. You know, you want the driver's eyes on the road in front of them, as opposed to constantly looking at signs off to the left and the right and blinking lights and all the rest, and have made some different -- this subcommittee has made some different recommendations there.

As it relates to the facial matching algorithm, this is probably where we'll spend most of our time. And we really do appreciate the comments from the public and privacy advocates in this area. We have some enhancements further selecting out the areas that we will talk about in just a second here.

But let me, you know, at a high level in our subcommittee launch tell you this, is that we are clearly focused on making sure that all persons -- irrespective of age, gender, ethnicity, diversity, color, just every single thing that's under the sun from the smallest demographic variables -- that the technology is actually doing what it says it's going to do. The DHS CBP is transparent about that. That numbers are being made public, that numbers are being preserved and used to inform the traveling public, and that as the technology grows and gets better, that we are able to focus more on those areas, and placing some onus and burden on DHS in terms of making sure that that happens.

Regardless of where that information comes from, regardless of the devices it comes from, making sure that DHS is that and CBP is that agency that is going to bring together that data so that it can be transparently viewed by the public. That is really where we focused a lot of our time efforts, and I think you'll see that in the paper and through some changes that I'll bring you -- talk to you about real quickly.

In terms of partners in data protection, you know, we really focused on a few things, right? The processes before the screening of individuals and facilitating that within the United States, both inside -- moving into the United States and egressing the U.S. We wanted to make sure -- and we actually call this out, and I'll go over it in a second. We wanted to make sure that we call out these pictures. Now we're not recommending they be used for business purposes, marketing purposes, all the rest. We're recommending strong protections against those items.

In addition, that they be used for, really, the clearance process, right? Are you who you say you are? Not for other law enforcement purposes. And once again, the Policy Committee makes those recommendations quite loudly, and we'll bring you to some of those changes to make it even more evident.

As it relates to usefulness of photographs, look, there are some different studies that need to be here, and throughout the paper, we do recommend -- and we have seen this, this is one of the great things about the timing of this. Through

our yearlong communications with CBP and DHS Privacy Office, we have seen many of those observations that we've made, either in July after our phone calls, be implemented actually now.

The November 14th PIA, the role of PIA on the [inaudible], I mean, we greatly applaud that. Taking up the separate PIAs, bringing them together, turning where we actually are, and showing us that you're listening to some of our recommendations, even if they are oral recommendations, that you're listening to some of those and baking them into the process is hugely helpful. We do think that there's a role for NIST to play. We do think that there is a definitive role for DHS S&T, Science & Technology, to play, especially as it relates to the technical specifications here, and wanted to make sure that DHS should -- all right, not like it may reach out, DHS should reach out to those agencies as we're talking about those very, very technical background types of items.

As it relates to the photographs, you know, really it was looking at about 8 1/2 to 10 1/2 years in terms of their trustworthiness, the accuracy in terms of being able to identify people there.

When we go ahead, and I'm going to have -- I'm actually going to come up -- let me come up there, and I'll see if this works. See if we can see here. Okay, this works. Okay. Can you hear me online? Yep. All right.

So what I'm going to do is we did call out some further enhancements, if you pay attention to the television monitors, and I will say this, is that the Policy Committee has met on these. We are in agreement on these. And we are -- wanted to make sure that folks were able to see those changes that had happened or some of those additions that had happened kind of in real time here before we -- before we go ahead and vote on things.

Oh, let's see. Most of those first changes, if they will come on -- there we go -- whatever page that is, page 8, really an ensuring accuracy perspective. All of these items that we are calling out further are -- they're already in the paper. What we wanted to do is make sure that, you know, look, there are reports out there about inaccuracy on facial recognition technology. The reports, quite honestly, that are all over the place in this, both in terms of the great accuracy and great strides that have been made, as well as inaccuracy of some of these technologies.

We want to make sure that DHS knows that it should take the lead to work with technical partners in this area, work with the different vendors of the biometric technology, contractually require some periodic reporting on the accuracy and effectiveness of the technologies, especially as it relates to individual personal factors and other demographic factors with an eye on continual improvement. So these will be part of the paper that we vote on today, a part of our policy perspective as we vote on it today, and they've been to the final -- final paper,

that is, well, at least to DHS.

The second area that I wanted to make sure that we had insight over was the different summary conclusions in this area. So, once again, making sure vendor requirements are made in regards to auditing around the requirements and performance of biometric systems, as well as other components of the governmental entities and really steadfastly working with this in DHS S&T. It appeared in other parts of the paper, one especially called out in this section to make sure that there's a minimization of disparity of accuracy and identification of persons of different race, color, ethnicity, age, sex, and other similar factors.

The second area that I did want to call out, and sorry I'm scrolling a little bit fast, was that we wanted to make sure that, look, in terms of the use of this onward data, it's not being used for marketing, other business purposes. That it is not being used for other governmental purposes -- law enforcement or intelligence purposes. It is used for the actual clearing/screening of the traveling public through those, you know, through those vectors by which they travel.

So those are some of the different changes that have been made, some of the enhancements where we pull out some of these further details from the Policy Committee. From Policy Committee side, did I miss anything? I might have when I was quickly scrolling. Did I miss -- no? Getting no mistakes there.

So what I would do is I'll return to my seat, but in the meantime, what I would do is turn it over to ask the question of the rest of the DPIAC committee in terms of any areas of items that you have questions on of the Policy Committee as we make -- the subcommittee makes the recommendation to the full committee that the paper be adopted, obviously, with these changes.

We also caught a few snarfs, as we always do. So it is now fairly snarf free. No guarantees though. Snarf? It is a massively technical term. Very, very technical term. But with that said, I think we'll turn it over to the DPIAC to be able to ask us, the subcommittee, any questions that it has.

MS. LISA J. SOTTO: Any questions for Chris and the subcommittee?

MS. SANDRA L. TAYLOR: Stand by for me, Lisa. I may have a question online.

MS. LISA J. SOTTO: Okay.

MS. SANDRA L. TAYLOR: No. It's Charles Palmer. He's fine. Okay.

DR. CHRISTOPHER PIERSON: So then -- so then, with that said, any other discussions, questions among the DPIAC? If not, I think, Lisa, as chairperson, the subcommittee would then ask for a move for a formal vote and approval by DPIAC.

MS. LISA J. SOTTO: Yep. All right. No questions? Yes?

MS. MARJORIE WEINBERGER: More of a comment, actually. Hi, I'm Marjorie Weinberger. More of comment because I think of these as substantive changes, not just snarf removal. I wonder if it makes sense for us to see it in advance of calling for a vote on it. If there had been changes, we scrolled through very quickly to the red changes in there. I didn't get a chance to read them. I certainly couldn't see them enough to do that. I don't really feel qualified then to make a vote on something that has such significant changes to it.

MS. SANDRA L. TAYLOR: We don't have to vote today. I mean, clearly, if there are any issues or concerns, I mean, we can table the vote until all of the committee members have had an opportunity to read through the report and can -- we do have some members from the public who would like to present comments. So we may take that into consideration as well. But we don't have to vote it today.

MS. LISA J. SOTTO: All right. That's a great comment, and we'll -- look, we want to make sure everybody is comfortable.

MS. SANDRA L. TAYLOR: Yes.

MS. LISA J. SOTTO: And you know, certainly this is important enough that let's take a little bit of a breather and give folks around the table time to review the changes which were made quickly in response to comments that we've received only in the last couple of days. So, yes, let's hold. And Sandy, you'll let us know procedurally how we can then move --

MS. SANDRA L. TAYLOR: Convene another meeting. It would have to be public again. I mean, we don't have to come together in person. We can do it via a conference call, but it has to be done in the public.

MS. LISA J. SOTTO: And you'll have appropriate notice in the Federal Register?

MS. SANDRA L. TAYLOR: Absolutely.

MS. LISA J. SOTTO: Okay, okay. All right. Thank you very much.

So let's then move forward unless any further comments, you know, please certainly make your questions known.

Okay. Let's move now to an update from Marc Rosenblum. Marc, please come forward. Marc is Deputy Assistant Secretary in the Office of Immigration Statistics, the DHS Office of Policy.

The Office of Immigration Statistics leads the collection and dissemination to Congress and the public of statistical information and analysis useful in evaluating the social, economic, environmental, and demographic impact of immigration laws, migration flows, and immigration enforcement. The office establishes standards of reliability and validity for the Department's immigration statistics.

Thank you very much for updating the committee.

Agenda Item: Immigration Data Initiative Update

MR. MARC ROSENBLUM: Thank you for having us. I also have Ryan Baugh here from my office, who handles our privacy work or is our lead on privacy stuff.

It looks like I think that our right slide show was out here on paper, but I think it's different up on the screen.

MS. SANDRA L. TAYLOR: We have it.

MR. MARC ROSENBLUM: Oh, that looks better. Good. Thank you.

So thank you very much to -- should I do that myself?

MS. LISA J. SOTTO: Yes, perfect.

MR. MARC ROSENBLUM: Sure, thank you. Thank you very much to the committee for the report that you will be giving us today. We've appreciated even the chance that we've had to look at it and the support that you've given us.

I wanted to quickly, and I know -- I'll be very quick. I wanted to walk you all through what the Immigration Data Integration Initiative is, the progress that we've made this year, and our goals for '19, and then I think, you know, we'll sort of -- we anticipate sort of accepting all of your recommendations and building that into our workflow.

So the IDII, the DHS Immigration Data Integration Initiative, responds to the problem that DHS immigration data remain dispersed across many different data systems, and those data systems are siloed. They don't -- the same individuals in the different data systems, it's hard to tell an individual in one data system is the same as that person in another data system. And frankly, very little progress has been made on that since the Department was stood up about 15 years ago.

You know, in an effort to bring all of these agencies together, the data still remain separate. And it creates all kinds of challenges for doing any kind of evidence-based policy-making, and it creates challenges for reporting and analysis. And so the vision of the IDII is to create a single, centralized environment in which the

data are linked at the person level for purposes of reporting and analysis so that we will have a single, authoritative set of linked immigration data that the Department -- stakeholders around the Department can rely on for operational research, reporting, and analysis.

And so there's three main lines of work that go into that. One is that we are working to create enterprise-level data standards so that all of the different systems around the Department will have common definitions. When we talk about both how terms are defined, what we mean by a removal, what we mean by an apprehension or an arrest, and then also how data are structured and formatted in the different data systems. So that's one line of work.

A second line of work is to make these person-level linkages across the different systems so that we can see an individual who's apprehended by Border Patrol and detained by ICE and makes an asylum claim before USCIS and then goes over to DOJ and has their proceeding adjudicated, that we can trace that person across those different systems and link those records.

And then the third line of work is to create -- is to put all of that data into a single IT environment and to create data tools where we can look at those records and the connections across them. And you know, briefly, that creates all kinds of operational efficiencies. We're not going to go in and restructure how the components collect data, but there are lots of operators who have to search multiple systems or input data multiple times, and down the road, this should mitigate some of those operational inefficiencies.

But the main effort, the main sort of benefits of the IDII are to be able to have faster and more comprehensive and more consistent reporting so that we can easily talk about, you know, all of those systems in a comprehensive way. And it has lots of implications for operational -- for analytic research. We can look end-to-end at how people move through the immigration enforcement system and the immigration benefit system and analyze those systems at sort of an enterprise level rather than system by system.

So this effort was initiated in late 2016. We -- by Secretary Johnson. We stood up an Executive Steering Committee that has representation from all of the immigration -- all of the operational components that have immigration equities and all of the headquarters components. And we received our first appropriation in the FY '18 -- or our first funding in the FY '18 Appropriations Act. And so we've actually, just in the last few months, began to -- we've begun to bring on some contract support, and we've hired our -- we just hired our first program manager.

She's actually in orientation right now I think in this building. Oh, there she is. Michelle Steinmetz is here. So we have our first IDII official hire now in the room. So we're excited to be really moving forward with this now that we've got some resources in place.

And so I'll briefly talk about the accomplishments that we've made in FY '18. One is that we have begun to publish enterprise data standards. This is a real grassroots effort where we work with the actual sort of business around the Department to collect information on exactly how terms are defined in all of these different systems and then sort of deconflict across the systems and come up with consensus standards.

So we've published so far 13 data standards. We have five more in process, and we'll probably publish about that number again, another dozen or so this year.

A second set of accomplishments is around sort of the IT work, and the main thing that we've done here is we have stood up an interim integrated IT environment where we have begun to place the linked data as we have begun to create these linkages across the different systems and begun to move the data a lot more efficiently into this linked environment. Historically, OIS, which is sort of the official -- which is the official recordkeeper for DHS immigration data, we've gone around the Department and picked up CDs from the operational components, and so we have now moved into, you know, the 1990s, and we're getting it electronically instead, which we're very excited about, and we've begun to get direct access to some of the systems so that we can build this more efficiently.

And we have been working closely with the Office of Privacy to make sure that we're doing this carefully and appropriately. So we did a privacy threshold analysis, and just I think on Friday, we finalized and published the privacy impact assessment that describes all this work. And Ryan and his colleagues in the Privacy Office did a ton of work to get that done. So we're really pleased that that's up on the website.

And we've also just been in discussions with S&T to get some support from one of their Centers of Excellence to help us to make sure that as we're building this dataset that we're mindful of re-identification threats that you guys talk about in your subcommittee report, although that's still in discussion. It's not something we've turned on yet, that effort to do that testing.

I think the most important thing for me to tell you about is what we've done to actually build this integrated dataset. And in short, what we've done is we've taken records from now 19 different systems across DHS and the Department of Justice, and we have for each of those systems connected the records at a person-centric level. And so we use a number of different identifiers because the different systems rely on a mix of identifiers. Some of them use a number. Some of them use FIN ID. Some of them are name and birth date.

And so we have come up with a careful methodology that allows us to go through a series of different data sorts and matches to make sure that we're matching

those records accurately, and we've done a lot of testing to look at our false positive and false negative rate. And we believe our accuracy rate is over 99 percent in that -- in building that person-level dataset. And these are the records -- or the data systems that are currently in there.

So, currently, as I said, we're collecting data from 19 different systems, covers 12.1 million unique individuals and 52 million events associated with those individuals. And the current data that we brought in are very much focused on the immigration enforcement system. So it's people who've been apprehended or arrested are sort of the -- or found inadmissible. That's sort of the scope of who goes into -- of what records we're focusing on as sort of the initial set of records.

And then we trace through every subsequent action, either in the enforcement system or the benefit system, that we can identify for those individuals to see what's happened to them after their arrest or their apprehension or their inadmissibility determination. But the plan is to expand that dataset, you know, with sort of all of the immigration data eventually so that we can do the full range of reporting and analytic work that the Department asks of us.

One important deliverable that we've used, that we have produced with this merged data is a report that we published in August on -- so this report looked at the population of aliens who were apprehended or found inadmissible on the Southwest border in 2014 and assesses where are they now, with "now' being as of the end of FY '17. So this is the first time the Department has had the capability to do that kind of reporting.

So of all those people who were encountered on the Southwest border, how many of them have been deported? How many of them have been ordered removed, but not had that removal ever executed? How many of them remain in proceedings? How many of them have been granted a benefit relief from removal?

So it's a very powerful analytic tool for the Department to understand sort of where the bottlenecks are in the system, how different people move through the system in different ways by linking these records across the different systems. And we've also provided a lot of support to -- a lot of analytic support to senior leadership to gain additional visibility in folks who continue to arrive at the border and to sort of understand how people continue to move through the system in different ways as a function of are they claiming asylum or not. You know, what happens to the asylum seekers versus the not asylum seekers?

So by linking these records, we get a lot more analytic insight into how the system functions, which obviously is why you guys are interested in it, appropriately. But you know, also why the Department should be doing it. So I will just conclude by telling you what we are hoping to accomplish this coming

year, this year, FY ‘19.

One of the things that we've been focused on, in addition to sort of the analytic advantages of linking these records, is to improve our reporting rhythm. Historically, OIS did reporting strictly on an annual basis. We, in FY '18, began reporting quarterly. We're still sort of firming up our ability to report quarterly and working on doing selective monthly reporting.

And then so we're moving to this monthly reporting rhythm. We're collecting use cases from around the Department. What are analytic products that our leadership is looking for and moving forward on delivering those analytic products. Those products require us to publish data standards so that we can, you know, sort of understand the terms that we're doing analysis on.

And then the big -- next big deliverable is that we would like to build a tool to allow stakeholders in the Department to search this merged data, to do sort of custom data pools that will allow you to query, you know, this merged data to ask questions like, you know, how many -- how many asylum seekers were there from country X in sector Y, you know, in time period Z? Things that currently are quite complex should become, you know, quite easy analytically to do with this merged data.

You know, again, with all of the concerns that that raises around this table about not allowing those cells to be too small, but with all of the sort of analytic power that comes to the Department and to researchers of being able to ask questions like that. So that will be the big deliverable this year is to create a tool that allows us to sort of look at this complex data at the person level and to produce custom tables and crosstabs that offer insight into how the system works.

Thank you.

MS. LISA J. SOTTO: Okay, terrific. Thank you so much. Let's take just one question from Mr. Sand, and then let's move on quickly to let Joanna present the paper.

Go ahead, Pete.

MR. PETER E. SAND: My name is Peter Sand. I have a question.

COURT REPORTER: Do you have a microphone?

MR. PETER E. SAND: I don't have the mike. I thought I’d just do it faster. So ask my question is, are there any questions which are unacceptable, that qualitatively do not fit in the question purpose? Are there taboo questions?

MR. MARC ROSENBLUM: So I'm not sure this is a totally direct answer, but let

me tell you one big taboo is that because we collect data both from DHS and from the Department of Justice, an overarching taboo is that we are not allowed to share that microdata with the DHS operational components because to do so is ex parte communication between EOIR and DOJ -- and DHS.

So any data that we share around the Department is anonymi. So, you know, we are providing support to operational components in terms of currently we're providing just summary tables, but our expectation is to provide anonymized data that will be totally de-identified because we're prohibited under our MOU with DOJ from sharing any PII. So that's an overarching taboo that we expect to stay in place.

I mean, there is strong legal demands that we not share PII around the Department. And then our -- and then whatever protections are attached today that we receive, like when we receive data on T and U and SIJ visa holders, those data have protections associated with them that would extend to any data sharing that we would do. So we preserve whatever protections come with the data and any sharing that we would do.

MS. LISA J. SOTTO: Okay, thank you very much.

Joanna Grama, who chaired our Technology Subcommittee, is going to present to the full committee the subcommittee's findings regarding privacy considerations in immigration data statistics. If there are no comments that cause us to revisit, we will then take a vote and accept the final paper.

Ms. Grama?

Agenda Item: Subcommittee Report -- Immigration Data Statistics

MS. JOANNA L. GRAMA: All right. Well, thank you, and I would like to echo the thanks to all my colleagues at the Privacy Office for your administration of the DPIAC, and also my thanks to the Technology Subcommittee that really hung in there for this one. So thank you.

Last September, so September 2017, the Technology Subcommittee was tasked with providing guidance on how to best disseminate statistical data. Specifically, we were looking at guidance for reporting purposes --

COURT REPORTER: I'm sorry. Can you fix it to your collar because it's --

MS. JOANNA L. GRAMA: We were also asked to provide guidance on information technology and policy perspectives about how the best practices -- best practices to communicate all these for statistical purposes. After some

communication with the Privacy Office, we determined we would refer back to the DPIAC guidance [inaudible].

And we really focused our query on what policy concerns should be addressed in the sort of statistical data dissemination of aggregate data. And you can read our report. We talked to a lot of people. We are not statistical experts, but we certainly got a schooling on the Technology Subcommittee about statistical best practices. We identified two high-level concerns that the Technology Subcommittee thought were important to address.

The first was that of data re-identification and testing for any statistical data [inaudible]. Closely related to that is the idea that even though these data for reporting purposes may be anonymi in the aggregate, and there is an inference that could be done looking at different datasets and combining datasets. And we're particularly concerned about inferences that could be made for enforcement action or discriminatory purposes.

And so that we would add to this project that we just be particularly mindful of re-identification and any intelligence information that could be made with the data.

That's it for the Technology Subcommittee. Thank you.

MS. LISA J. SOTTO: Any comments or questions from the full committee?

MS. SANDRA L. TAYLOR: So is it possible for Joanna to outline the recommendations that you're -- for the full committee?

MS. JOANNA L. GRAMA: Sure. Sure, our recommendation for the OIS to conduct data re-identification testing to determine whether any publicly provided statistical information could be positively re-identified to a unique individual, and then that we also recommend that the OIS consider that the anonymization and aggregation and [inaudible] actions alone [inaudible] privacy and data sharing agreement of other readily identifiable variables, such as demographic data or geographic data, should be included with the data file.

MS. LISA J. SOTTO: Do we have any questions from anyone on the full committee?

[No response.]

MS. LISA J. SOTTO: I think we can, if I can ask for a motion to accept the paper? Any motion?

[Motion.]

MS. LISA J. SOTTO: Do we have a second?

[Second.]

MS. LISA J. SOTTO: Okay. Please say aye if you agree.

[A chorus of ayes.]

MS. LISA J. SOTTO: Any nays?

[No response.]

MS. LISA J. SOTTO: Any abstentions?

[No response.]

MS. LISA J. SOTTO: Okay. I think we have a paper. We have a formal paper. Thank you very much, and thank you so much to the Technology Subcommittee. And thank you to our panel.

MS. SANDRA L. TAYLOR: I think we have one individual who would like to provide comment to the full committee. So I'm actually going to call him up now.

Agenda Item: Public Comment

MR. JEREMY SCOTT: Good afternoon. Can you hear me okay? Excellent.

My name is Jeremy Scott. I'm an attorney with the Electronic Privacy Information Center. We are a public interest organization. We focus on emerging privacy and civil liberty issues.

Before I begin, I want to thank the committee for having this public meeting and also taking comments on your report regarding facial recognition, and I also would like to appreciate the CBP and officials at CBP on their privacy work with respect to the Biometric Entry/Exit Program.

But I do want to point out a few issues about the Biometric Entry/Exit Program to emphasize why this is such a privacy issue, and I know we're running short on time. So I'll keep these comments short.

First, facial recognition is the biometric most easily used for surveillance. As the committee's report actually notes, facial recognition can be done to identify people in photos, in videos, or in real time, and now CBP is building the infrastructure that can easily be used for other surveillance purposes.

CBP created an opt-out program, not an opt-in program for American travelers, and it's not even really the opt-out program. CBP builds the facial recognition

gallery regardless of whether I want to participate in that program or not.

Third, and perhaps most importantly, there are no Federal laws that provide safeguards needed to address the collection, the use, the disclosure, and the retention of biometric data, particularly for facial recognition purposes, and there's no safeguards generally to make sure that the program does not expand beyond its original purpose.

The traveling public must rely on DHS and CBP's policies and procedures to make -- to ensure that the program doesn't expand, and these policies and procedures can easily be changed without appropriate laws in place.

Fourth, the Biometric Entry/Exit Program is an example of how data collected for one purpose can be used for another. CBP saw fit to take the images submitted to the State Department in order to obtain a passport ID and use that information, those images to conduct facial recognition.

This is known as "mission creep," as I'm sure most of you are familiar with. And it's interesting that this program was essentially built on what I would say is an example of mission creep. And without laws in place, there is no real kind of safeguards to prevent this program to expanding as another example of mission creep.

Those are the main points I wanted to make. I'll just point out two other quick things that come to mind. One, since there was submission of a report today, I would like to just highlight the fact that the DHS Office of Inspector General report found that CBP encountered various technical and operational challenges that limited biometric confirmation. So it isn't like a perfectly working, smooth program.

And secondly, in the experience of EPIC’s executive director, the alternative method was not just a simple check of the passport via a manual check but involved actually questions about his travel. So I'd like to push back against the idea that this is always strictly a manual check real quick of the ID for those people who actually opt out of the facial recognition part. That hasn't been the experience necessarily, and this was a recent occurrence in the last week or two.

And with that, I'll end my comments.

MS. LISA J. SOTTO: Thank you so much. And we really do very much appreciate written submission. And we have not only read it, but we have taken some of the comments to heart, as you can see by the last-minute changes.

I'll leave the dearth of Federal legislation to Congress. But we will absolutely take all of your comments today under consideration, as well as the comments that were submitted.

So, Chris, anything to add?

DR. CHRISTOPHER PIERSON: No.

MS. LISA J. SOTTO: Okay. Thank you very much.

MS. SANDRA L. TAYLOR: Thank you, Jeremy. Thank you very much.

Jim Adler has a question on the phone. He's one of our members. Can you open up the line for me, please?

OPERATOR: The line is open. Mr. Adler, please go ahead.

MR. JAMES ADLER: Yes. Can everyone hear me?

MS. SANDRA L. TAYLOR: Yes.

MR. JAMES ADLER: Okay. My question just followed up on some of the previous thoughts around the facial recognition technology and the purpose specification. It sounds like you've heard those concerns and are taking them to heart, which I greatly appreciate giving us time to incorporate these new drafts of the recommendations for a later vote.

So my concerns have been addressed. So thank you.

MS. SANDRA L. TAYLOR: Thank you, Jim. Do we have any questions on the phone?

OPERATOR: The lines are open are if you wish to ask a question.

[No response.]

MS. SANDRA L. TAYLOR: Do we have any questions from any members in the room?

MS. LISA J. SOTTO: Marjorie, please.

MS. MARJORIE WEINBERGER: Thank you. My name is Marjorie Weinberger.

I'm asking actually if the Privacy Office would be willing to share with us the Inspector General report that was referenced by the gentleman from EPIC. It might be interesting for us to see recent reporting on the issue.

MS. SANDRA L. TAYLOR: Yeah, we'll share it.

MS. MARJORIE WEINBERGER: Thank you.

Agenda Item: Meeting Adjourned

MS. LISA J. SOTTO: Any other comments and questions before we close? And we will be getting together in the near future to vote on the revisions to the Policy Subcommittee's paper.

Okay. With that, we will look to close the meeting. Many thanks to our speakers, our panelists, our committee members, and members of the public for participating. We very, very much appreciate it.

This concludes the public portion of our meeting. We are grateful for your interest, and we encourage you to take a look at the website to follow the committee's work, dhs.gov/privacy.

This meeting is adjourned.

MS. SANDRA L. TAYLOR: Thank you.

[Whereupon, at 3:57 p.m., the meeting was adjourned.]