1 DEPARTMENT OF HOMELAND SECURITY

2 DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

3 PUBLIC MEETING

4

5

6

7

8

9

10

11 Tuesday, July 17, 2012

12 1:00 p.m.

13

14

15

16

17

18

19

20 United States Access Board

21 1331 F Street, N.W., 8th Floor

22 Washington, D.C. 20004-1111

PARTICIPANTS

SHANNON BALLARD, DESIGNATED FEDERAL OFFICIAL
LISA J. SOTTO, CHAIRMAN
SUZANNE BARBER
J. HOWARD BEALES III
CRAIG BENNETT
JAMES BYRNE
MARY ELLEN CALLAHAN
AARON CASAVANT
JAMIE DANKER
PAT DIBARI
RENARD FRANCOIS
MICHAEL FROOMKIN
MELODI GATES
JOANNA GRAMA
JEEWON KIM
LINDA KOONTZ
JOANNE MCNABB
LISA NELSON
GREG NOJEIM
LYDIA PARNES
CHRISTOPHER PIERSON

1 PARTICIPANTS (CONTINUED)
2 TRACY PULITO
3 MARILYN SCOTT-PEREZ
4 BARRY STEINHARDT
5 DON TRINER
6 MARJORIE WEINBERGER
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

MS. BALLARD: Good afternoon. My name is Shannon Ballard. I am the Designated Federal Official for the Data Privacy and Integrity Advisory Committee.

And I want to say that everything now is on the record, and I'd like to turn it over to Lisa Sotto, the chair, and have a great meeting.

Thank you.

MS. SOTTO: Thank you very much, Shannon. Thank you, Shannon.

I am delighted to welcome this committee to what is the third meeting of this 2012 fiscal year for the Government. I'd like to just remind everybody at this early stage to silence your cell phones. I just turned mine off.

And I would like to extend a special welcome to our new committee members: Suzanne Barber, Jeewon Kim, Melodi Gates, Linda Koontz, Marjorie Weinberger. Let's see, going this way --

MS. BALLARD: Tracy.

MS. SOTTO: Tracy Pulito, Jim Byrne, Craig Bennett, and everybody else is an extant member.

So, really, this is a very important committee,

and we have important work to do to assist Mary Ellen and her crew. I think you'll find it to be also personally rewarding, as I have over the last several years.

We do expect lots of input from you and a good commitment to the work we do. I know I've seen some of you in action this morning, and I have no doubt that your commitment is real. So thank you very much for that.

We engage on this committee in really open dialogue, free-flowing dialogue. So, typically, what we do is if you have a question, we put up our table tents on the desk, and I'll call on you in order of lifting -- of raising your table tents.

For any interested parties, the Federal Register notice to apply for DPIAC membership was published on June 22nd. I know that some members of the committee need to reapply if they want to be on the committee again. The process closes on July 23rd. So I would urge you to go ahead and reapply.

We have reserved time for public comments from 3:45 p.m. to 4:15 p.m. So if you're interested, please

sign up. There's a table. I think it's right at the end of the room. Keep in mind that the public comment period might begin earlier if our discussion is accelerated.

So, with that, I would like to welcome and it gives me real pleasure to welcome Mary Ellen Callahan. Mary Ellen is the Chief Privacy Officer of the Department of Homeland Security. In her role as Chief Privacy Officer, Ms. Callahan is responsible for evaluating department-wide programs, systems, technologies, and rule-makings for potential privacy impact and for providing mitigation strategies to reduce any privacy impact.

Prior to joining the department in March of '09, Ms. Callahan specialized in privacy and data security with the law firm of Hogan & Hartson, and she was also co-chair of the Online Privacy Alliance. In addition, she was vice chair of the ABA's Antitrust Division Privacy and Information Security Committee.

Together with the Privacy Office, Ms. Callahan is responsible for privacy across DHS and also has the honor of serving as the department's Chief Freedom of

Information Act Officer.

With that, I would ask you please to proceed and thank you very much for joining us.

MS. CALLAHAN: Thank you very much, Lisa. Mic's okay?

I want to thank all of the committee members who are here today, particularly the new ones. I want to welcome you aboard. It is -- we have new members here. This is also a new location for the DPIAC. It is for the past several years, the department has looked to use exclusively Federal facilities. And so, we have been on quite a sojourn throughout the District of Columbia and, actually, Virginia, now that I think about it.

And we have gone to many locations, but I think this is actually a really great space. So I really appreciate the Access Board's flexibility in allowing us to be here today, and I look forward to working in this space.

In addition, this is, I believe, Lisa's first official meeting as chair, and we also have a new Designated Federal Official with Shannon Ballard, and

so we appreciate all of you. And so, for the new members, don't think that, oh, my God, everyone knows what's going on.

Not necessarily. Lisa has been, actually, one of the original members of the DPIAC and so has been longstanding and was vice chair earlier. But we're thrilled to have her on in her new role as chair.

I also wanted to mention that in slightly inconsistent practice from the previous few times, this meeting will be transcribed. So it will be both transcribed, and there will also be minutes. So I'm just mentioning that for transparency because that's part of my job.

But I wanted to thank you all and to welcome you all. For those who are interested in the audience, the new members' biographies, brief synopses are available at the registration table or just adjacent to it.

So, for your information, I give kind of an overview of what's happened in the department and specifically with the department and privacy since we've last met, which was in early December 2011. And so, I'll be going through a series of different issues.

I'll try to tie it together with things we've done in the past. But if you have questions, again, as Lisa said, this is a very free-flowing committee, and I expect to see table tents go up as I speak.

Following my ordinarily long-winded discussion of what the department does and is doing in privacy, we'll have my colleague Don Triner, who is the Director of Operations Coordination for the department's Office of Operations Coordination and Planning, will be joined with the Associate Director for Privacy Compliance Reviews Jamie Danker. They're going to talk to you about the National Operations Center Social Media Situational Awareness Initiative.

So we've talked about this a couple of different times. Don was supposed to testify, if you remember, in December. But due to the debate on the paper, we had to postpone it.

The social media initiative, just for your information, is a process by which the National Operations Center, or NOC, works together to go and try to leverage social media for situational awareness of homeland security issues. Don is going to talk about

that and also talk about the privacy protections embedded into that process, and Jamie is going to talk about the recently completed privacy compliance review.

We've done four different compliance reviews of the social media situational awareness that are available on our Web site so that we can talk about kind of how we embed privacy into the life cycle of the department's activities.

And then continuing with our schedule of having component Privacy Officers appear before the DPIAC, we'll be joined by members of the U.S. Coast Guard. Commander Pat Dibari, who is Deputy of the Office of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance -- and apparently, it's C4ISR -- and Commandant Marilyn Scott-Perez, who is the Chief of the Office of Information Management, aka the component Privacy Officer and the component FOIA officer, are going to discuss maritime biometrics and some of the work that the Coast Guard has done specifically with regard to their Biometrics at Sea program.

So we're going to have that to do.

1 So now I'm going to turn to the Privacy Office's
2 accomplishments, ongoing activities, and future plans.
3 If you may recall, last year I mentioned that we had
4 launched an initiative to examine the Privacy Office's
5 strategic plan to assess how we are aligned with the
6 department's Quadrennial Homeland Security Review,
7 known as QHSR.
8 And I'm sorry. For the new people, there will be
9 a lot of acronyms, but I'll try to define them ahead of
10 time. But the Quadrennial Homeland Security Review
11 kind of every 4 years takes a snapshot and looks at
12 what homeland security's mission is.
13 So we launched an initiative with the Privacy
14 Office to align our strategic plan with the Quadrennial
15 Homeland Security Review and to basically chart a
16 course for future accomplishments. As part of that
17 process, I had a working group that worked on the
18 strategic plan looking across the department and across
19 the Federal Government in terms of how to position our
20 office.
21 I also surveyed my entire staff to ensure that all
22 their views and all the different levels were

1 considered as the old version of the plan was revised.
2 I also held an offsite with my senior leadership to
3 revise the office's strategic goals and objectives.
4 And we have subsequently released the strategic
5 plan. I believe there are copies in the back. If
6 there are not, they're available on our Web site.
7 What we've done is we've realigned our goals for
8 our fiscal year and beyond to be harmonized with the
9 QHSR, but also to show that we clearly communicate our
10 aims going forward. There is a copy at the
11 registration and on the Web site, as I mentioned, and
12 I'm going to define what it is.
13 We have five major goals. And throughout my
14 presentation, I'll define it. So we were working on
15 that.
16 So in addition to the strategic plan, which we
17 launched on January 20th of this year, we also began to
18 examine the staff structure to ensure that it was
19 organized as effectively as possible to carry out these
20 new goals and, candidly, to be nimble enough to deal
21 with the department overall. The structure had not
22 been looked at in a few years. And candidly, this has

been kind of an evolutionary process with the department.

My office in particular, I said this when I started, it felt a little bit like a start-up, and it was kind of structured a little bit like a start-up, like so-and-so came in. So, okay, this is what they're doing, and this is who they're reporting to.

So what we tried to do is to redesign the new organizational structure to accomplish three objectives. First, to establish new teams allying with each of the five strategic goals. We then were able to have our supervisors and our staff quickly map out the current projects and policy initiatives and have them be prioritized associated with the strategic plan.

We also looked to delegate supervisory responsibility among existing senior staff. I have an incredibly rich, diverse, talented group of senior staff in my office. And the changes we'll make are SES, or Senior Executive Service, leadership be more nimble, which are the Privacy Officer and the Deputy Privacy Officer and the Deputy Chief FOIA Officer.

Allow us to be more nimble and allow the deputies

to spend more time coordinating with partners outside of our office while allowing, as I said, several seasoned GS-15 employees to have increased management skills and a chance to diversify their own skills. Furthermore, the third goal was to create new leadership opportunities and increase staff accountability.

The new reporting structure has clarified and brought increased focus to the portfolios of each of our Privacy Office staff. It's also created opportunities for more junior staff to take additional responsibilities and expand their skills with cross-cutting working groups on subject matter expertise, including social media, information sharing, international issues, the types of issues that cut across several of the different groups, but that we also have the ability to have new leaders charging with that.

So, as I mentioned, there are five strategic goals that are associated with our four divisions, which are the first strategic goal is to encourage privacy policy development and growth.

The second strategic goal is advocacy. This is part of the advocacy, actually. But also to reach out with privacy advocates and also reach out internationally and to our interagency colleagues.

The third strategic goal is compliance. And by that, I mean both privacy compliance and making sure that we're consistent privacy policy, but also FOIA transparency compliance.

The fourth strategic goal is a new one that I'm going to spend some time talking about a little bit, but it's privacy oversight. How do we make sure what we're saying is the truth? How do we make sure what we promise is what we're doing? And to take a look at that.

And then the fifth goal I think is an important one that I hope you guys will recognize, which is how do we develop our employees? How do we work on employee development, employee sustainability, employee growth and opportunities?

And so, with those five goals, we've reorganized the office to have -- to kind of follow along in the order of the goals. The first one is actually privacy

policy and advocacy team that's combined because a lot of the policy is going to influence the advocacy and vice versa.

That team is led by Helen Foster, and its main responsibilities include fostering a culture of privacy and transparency, demonstrating leadership through policy and partnerships, and providing outreach, education, training, and reports in order to promote privacy and openness in homeland security.

The second group aligns with the third goal of the strategic plan, which is privacy compliance. That's led by Becky Richards, our Senior Director for Privacy Compliance. And its main responsibilities are ensuring that DHS complies with Federal privacy laws and policies and adheres to the fair information practice principles.

The fourth group is also associated with the third goal of the strategic plan, which is the Freedom of Information Act portion of the office, led by Deputy Chief FOIA Officer Delores Barber, who is in the process of hiring a Senior Director for FOIA to match the others in the office. The FOIA team has the main

1 responsibilities for ensuring that DHS complies with
2 Federal disclosure laws and policies.
3 The fourth group is oversight, led by Martha
4 Landesberg, whose main responsibilities include privacy
5 compliance reviews, some of which you'll hear about
6 today, privacy investigations, privacy incident or data
7 breach responses, and privacy complaint handling and
8 redress.
9 The fifth group is our administrative team, known
10 as the PACT, which goes and knits us all together, and
11 it's also where our fifth goal in terms of employee
12 responsibility will also be housed.
13 So we're very excited about the strategic plan.
14 It's been -- from an operational implementation
15 perspective has been great, and I think it's really
16 helped mature the office and get into a circumstance
17 where the office and its responsibilities are less
18 personality driven and more subject matter driven. So
19 we're really excited about that.
20 We have other initiatives associated with
21 efficiency and sustainability. Small as my office is,
22 with 45 full-time employees, we have another

1 opportunity to identify savings in the next year, which
2 is that we're going to be relocating our offices to
3 downtown Washington, D.C., effective August 1st. It's
4 where the Technology Committee met earlier today.
5 It is -- we're very excited about it. It's going
6 to be good. We're going to be sharing space with more
7 DHS entities. We won't have to walk 6 blocks to get to
8 a SCIF. And it's going to be a good circumstance.
9 We currently have more space than we need for our
10 staff, and that's made us have to pay more for it. But
11 we also can't downsize because it's a full floor in
12 Rosslyn. But we're going to be able to reduce our
13 office footprint, contain costs by moving to a smaller
14 and more modern space, and we're going to be able to
15 leverage some of the DHS synergies as well. So we're
16 really excited about that.
17 Speaking of sustainability and strategic plan,
18 several of you may know that my longtime deputy John
19 Kropf departed Federal service at the end of January,
20 shortly after we launched the strategic plan. And I
21 actually couldn't have gotten the strategic plan done
22 without John and without my chief of staff, Jordan

Gottfried.

But John had a phenomenal opportunity to take in the private sector and so has left Federal service. And it was sad for us, but it was a great opportunity with the strategic plan coming in to have some of the more senior staff take real leadership roles. And then we also went out and solicited to get a new senior executive status person to come in.

We've been incredibly fortunate to hire Jonathan Cantor, the former Chief Privacy Officer of the Department of Commerce and the former Chief Privacy Officer for the Social Security Administration, to come and join the department as my deputy. So we're really excited about that, and we think it's going to be a great opportunity.

And we're looking to learn from Jonathan, and I know he's excited about working with our office as well on the complex issues that the department deals with every day.

So, speaking of that, let's talk a little substance for a second. I'm going to talk about what the office is doing in order of the strategic plan. If

1 you notice a theme here, we're going to talk about
2 policy and advocacy first.
3 First, with regard to training, right? That's
4 kind of a core element. You've got to make sure that
5 people know what they're doing before we can go and
6 make sure that they're complying with it.
7 So we have a new online privacy course. We've
8 talked about this a few times, but we're very happy
9 that we finally were able to implement a brand-new
10 mandatory online privacy awareness course across the
11 department. We just launched it in early June, and
12 it's been very successful.
13 Participant survey results have been very
14 positive, and we've had a lot of people indicate that
15 it, indeed, is both informative and relevant to their
16 job. So that's what we want to do is really make it
17 relevant to the user.
18 We've also been able to work on some interagency
19 training and processes. Under the aegis of the CIO
20 Council Privacy Committee, of which I am a co-chair,
21 Steve Richards, our Associate Director for
22 Communications and Training, co-presented a workshop on

1 privacy training and awareness best practices in May to
2 over 135 privacy staff from across the Federal
3 Government.
4 Steve also created a Web site on an internal
5 Government portal to go and provide the training and be
6 able to leverage best practices for all the Federal
7 Privacy Officers to share and obtain resources so that
8 they can all create cultures of privacy within their
9 agencies without having to reinvent the wheel.
10 Particularly in a fiscally constrained environment, we
11 thought that that was a very good use of our time.
12 We are also in the process of developing a
13 comprehensive review of all privacy-related training
14 here at DHS to identify gaps and to develop new and/or
15 improve existing course work. We want to make sure
16 that we standardize the training across the agency and,
17 where possible, make it available online. All good
18 goals, hopefully, that you'll agree.
19 We also worked on some privacy compliance training
20 for the department and also for the Federal Government.
21 On June 20th, we held our sixth annual compliance
22 workshop that was attended by 221 people from 40

1 different agencies. It was a really great opportunity.
2 It's the only annual training available to Federal
3 practitioners that focuses on Federal privacy
4 compliance -- on the Privacy Act, on the E-Gov Act, on
5 FISMA -- and making sure that we understand that.
6 Our compliance group offered training on those
7 issues. It also talked about, in addition to the
8 statutes, the new NIST 800-53 Appendix J, which I'm
9 going to mention briefly, and provided practical
10 training on how to read a system of records notice,
11 which I probably should have sat in on that training on
12 that one.
13 We've also been active with some public outreach.
14 As you know, I have quarterly outreach meetings with
15 privacy advocates and held two of those, one in March
16 and one in June of this year.
17 We also have an annual Privacy Office speaker
18 series to talk about emerging privacy issues. If you
19 recall, this past year was the first time we had a
20 theme that ran throughout the entire year, which was
21 cybersecurity. And we opened up the series to all
22 Federal workers and contractors. It's been quite

1 successful, with over 100 people attending each event.
2 And there have been two workshops since December.
3 One on January 11th, which provided an overview of the
4 operational cybersecurity program and system known as
5 Einstein, or NCPS, and the planned strategy for the
6 future of cybersecurity protections across the Federal
7 Government. One of the speakers at that event was
8 Brendan Goode, who the Cybersecurity Subcommittee knows
9 quite well. And that was very well received.
10 And then on April 15th, we had three experts on
11 virtual worlds discuss the many applications of virtual
12 worlds and their impact on privacy, as well as a
13 history of a real Panopticon prison in Philadelphia,
14 which is the old prison that is in the middle of
15 downtown -- what is downtown Philadelphia now. And
16 it's -- what's it called?
17 Eastern State. Eastern State Prison that was
18 built in the 1700s, and it was this really interesting
19 sociological theory on kind of if everyone is in
20 solitary, will they get better? But they're watched
21 all the time. That's the Panopticon element of it.
22 It's a really interesting presentation and really

1 interesting way of thinking about how has privacy
2 evolved and what did it mean in the 1700s and what does
3 it mean now. So it was really very interesting
4 presentations.
5 We're going to continue the speaker series next
6 year with new thematic topics.
7 We also -- as this committee is aware, we've been
8 working with State and local fusion centers for quite
9 some time, and that work continues. Since our last
10 meeting, our in-person training program has visited
11 fusion centers in Alaska, Colorado, Connecticut, Iowa,
12 Minnesota, Oregon, Wisconsin, and right here in D.C.,
13 training over 200 State and local fusion center
14 representatives on privacy and civil rights and civil
15 liberties, combining with our Office for Civil Rights
16 and Civil Liberties.
17 And we have hit more than half of the fusion
18 centers with this kind of in-depth training while we
19 also, as you may recall, have trained all of the
20 individual privacy and civil liberties officers in the
21 71 operational fusion centers.
22 We are also going to be planning on a conference

here in Washington to work with those privacy and civil liberties officers there in the fusion centers to help update, again, share best practices, see how things are going on. There has been some turnover since we last saw them about 14 months ago.

We also participated for the fifth year in a row in the national fusion center conference in Phoenix, Arizona. This year, the conference was scaled back to focus on training. Therefore, our Privacy Office staff participated in a number of the training sessions, among other things, on the challenges of implementing their privacy policies and on the use of social media, which is a very worthwhile implementation on our part.

With regard to our work internationally, we have several results of note that I want to highlight. On June 28th, in coordination with the Department of Justice, Public Safety Canada, and Justice Canada, my office led efforts to develop and now launch a joint statement of privacy principles that will guide and inform the U.S./Canadian information-sharing initiatives.

As you all may recall, the U.S./Canada Beyond the

1 Border declaration was announced in February 2011 and
2 articulated a shared vision where both countries work
3 together to address threats at the earliest point
4 possible while facilitating the legitimate movement of
5 peoples, goods, and services into our countries and
6 across our shared border.
7 The joint privacy principles, as I said, announced
8 late last month, are based on commonly understood
9 privacy protections and fair information practice
10 principles, such as the OECD privacy guidelines, and
11 are consistent with the laws in each country.
12 My office will continue engagement with
13 stakeholders to ensure effective implementation of the
14 principles to all the Beyond the Border initiatives.
15 We think it's a very important statement with regard to
16 the Beyond the Border program.
17 In addition, we've talked about the U.S./EU
18 passenger name record agreement. We had the Deputy
19 Secretary appear before this committee last year. On
20 December 14th, Deputy Secretary Lute signed a new
21 passenger name record agreement with the United States
22 and the European Union.

The agreement passed the Council of the European Union with strong support and was ratified by the European Parliament on April 19, 2012. Having been then approved by the Justice and Home Affairs ministers on April 26, 2012 -- and if anyone wants to talk about EU process, come and let me know. It's byzantine at best.

But the PNR agreement reaffirms our commitment to extend essential security arrangements and protect individual liberty across the breadth of the U.S./EU relationship. My office, CBP privacy, and CBP overall will continue to ensure compliance with our commitments in that agreement.

Other ongoing projects in the international space. The Privacy Office continues to work on the interagency negotiation sessions on a U.S./EU umbrella agreement that would provide a framework for mutual recognition of our privacy systems to facilitate the exchange of law enforcement information.

The Privacy Office also continues to contribute to the department discussion on the development of information-sharing initiatives under the five country

1 conference, which is a forum of cooperation for
2 migration and border security between the countries of
3 Australia, Canada, New Zealand, the UK, and the United
4 States.
5 Privacy Office staff reviews the five CCs. That's
6 what it's called, the information-sharing agreements,
7 to ensure consistency with privacy law and policy, as
8 well as transparency through amendments to the privacy
9 impact assessments.
10 The Privacy Office also continues to support the
11 department's implementation of preventing and combating
12 serious crimes agreements, which are required for any
13 country who's participating in the Visa Waiver Program.
14 We're also engaging those partners to enhance the
15 understanding of U.S. privacy framework and DHS privacy
16 policy regarding information sharing under the
17 Preventing and Combating Serious Crimes Initiative.
18 We also have been making significant contributions
19 to the OECD's Working Group for Information Security
20 and Privacy and adjacent volunteer group, which is
21 reviewing the 1980 OECD privacy guidelines, cooperation
22 on enforcement of privacy law, and the upcoming review

of the OECD guidelines on information and network security, which is essentially cybersecurity. And we've been working to make sure that any changes be consistent with FOIA, the Privacy Act, the E-Gov Act, and OMB guidance for the public sector.

We are also leading a privacy training group under the CIO International Privacy Subcommittee, where efforts are underway to create a briefing on international privacy issues for the interagency community and consider ways to push out privacy best practices to our international partners.

We've also had a series of meetings with interagency and international partners on privacy framework, including from Canada, the EU, Finland, Germany, Ukraine, and Article 2 working group. So we're still working on outreach elements on that as well.

In August, we're going to be participating in the first Department of Homeland Security sponsored training program, titled "Understanding and Representing DHS Overseas." As I mentioned in previous updates, over the past 18 months, the Privacy Office

has been contributing to the development of this training session targeted at DHS officials being deployed overseas.

The Privacy Office will use the opportunity to convey a combination of knowledge and skills to enhance on-the-job performance to allow internationally posted employees to spot potential foreign policy issues brought about by misunderstandings about the U.S. privacy framework, DHS privacy policies, or other misperceptions about DHS information-sharing writ large.

Our goal is to provide a high-level overview of U.S. privacy law and policy to those outbound attaches and to raise awareness of the global privacy policy issues that could impact DHS missions and objectives.

In addition to some of the international work, we've had a lot of domestic revisions and maturations on that side. In March, we published a completely revised version of our handbook for safeguarding sensitive personally identifiable information, which sets minimum standards for how department personnel should handle sensitive PII in paper and electronic

1 form during their everyday work activities at the
2 department.
3 Included in this revision are best practices for
4 handling sensitive PII while teleworking, which, of
5 course, as you know, has become more common throughout
6 the Federal Government.
7 Later this month, I will testify on the state of
8 Federal privacy and data security law before the Senate
9 Subcommittee on Oversight and Government Management,
10 which is under the Senate Homeland Security and
11 Government Affairs Committee. The hearing will examine
12 the Privacy Act, the E-Government Act, and related
13 privacy laws to ensure that they effectively protect
14 privacy in the 21st century. I've been invited to
15 provide context based on my experience serving as the
16 department's Chief Privacy Officer.
17 That was all policy and advocacy. Now we're going
18 to switch briefly to compliance, which is I'm going to
19 quiz you what goal is compliance?
20 Renard?
21 MR. FRANCOIS: To make sure that we comply with --
22 MS. CALLAHAN: No, what's the number? It's three.

It's the third one. We got the third one. I'm going to quiz you.

MR. FRANCOIS: I'll leave the room.

(Laughter.)

MS. CALLAHAN: Since our last meeting in December, the compliance group has approved 475 privacy threshold analyses. I also have approved 29 PIAs and published 2 system of records notices.

Overall, our FISMA privacy score has increased to 82 percent for privacy impact assessments and 95 percent for SORNs. The scores that are reported to OMB are not static because new systems come online, and old ones are retired and so on. But we have seen an increase in the PIAs, 2 percent in this calendar year.

We're also very pleased to highlight that during this reporting period, FEMA got 100 percent compliance for both its PIAs and its SORNs, thanks to the leadership of the FEMA Privacy Officer Eric Leckey, who is familiar to many of you.

We have continued to build privacy into the department's security process. In June, the reporting for IT security has begun to color code the privacy

scores for PTAs. The coding of the PTAs will highlight where improvement is needed for component executives.

In October, the PIA score will start to be color coded. Scores below 70 percent will be red, 80 percent for yellow, 90 percent for green. I don't know what color Eric will be, and I have a couple other components that I'd like to give them a color. So --

(Laughter.)

MS. CALLAHAN: I want to highlight two key privacy impact assessments that I think will be of interest to the department or, excuse me, to the committee. We spent a lot of time developing where the Customs and Border Protection, CBP. I realized I used that acronym earlier without defining it. But Customs and Border Protection, their automated targeting system and their analytical framework for intelligence.

Both of these systems pose new and interesting privacy issues because they ingest data from source systems and then process that data. The department very much used some of the guidance that was provided in the DPIAC's 2011 paper on information handling to help inform some of the decisions we are making in the

1 systems that we are ingesting.
2 But I would like just to note that the federated
3 search concept has not yet been launched by the
4 department. So it's not -- we did not take all of the
5 thoughts or recommendations in the paper.
6 Both the system of records notice were out for
7 comment. So we received comments on both programs, and
8 we are in the process of responding to that through the
9 final rule process. Those should be published,
10 hopefully, shortly.
11 And finally, the Compliance Office is in the
12 hiring phase. Two of our compliance employees have
13 moved on. We've brought on a new employee, Dayo Simms,
14 from Social Security Administration. And you notice
15 that I'm taking the people from Social Security
16 Administration, and we're looking to hire two more. So
17 having the word out.
18 I turn now to the FOIA side of compliance, which
19 is the, again, third goal in our new strategic plan. I
20 issued a memorandum in January, entitled "Government
21 Openness" -- the Department of Homeland Security
22 applies both the letter and spirit of the Freedom of

1 Information Act -- which reaffirmed the department's
2 commitment to openness and transparency.
3 I also then issued a policy memorandum to help
4 support intra- and interagency collaboration on FOIA
5 requests to how to implement the new Department of
6 Justice recommendations on how to handle referrals,
7 consultations, and coordination. The policy encourages
8 components to leverage opportunities to more
9 efficiently handle those consultations electronically
10 or establishing guidelines or protocols to more quickly
11 deal with circumstances where more than one component
12 or agency has material that's responsive to the FOIA.
13 In March, Secretary Napolitano announced the
14 department's recognition of Sunshine Week by
15 recommitting to the letter and spirit of the FOIA and
16 by promoting -- continuing to promote transparency and
17 openness.
18 The DHS FOIA office has also been working on a
19 series of training, including a February session to
20 match my memorandum and to help implement the
21 Department of Justice new guidelines on consultations,
22 referrals, and coordination. And we also in April

received an especially tailored training from the Office of Government Information Services, which is a new organization scheduled in NARA to help the ombudsman for FOIA processing. The training was on alternative dispute resolutions, and a repeat session is scheduled for later this summer.

DHS FOIA launched a new Web site in April with an eye towards better educating the public about the FOIA process and reconceptualized to maximize usability. The site featured a simplified menu and graphic links to rich content, and the reorganized DHS online FOIA library, which is a really important element and has really expanded significantly in the past 3 years, helps bring together documents by type, directives, instructions, frequently requested records, with an index page that helps people find it.

Ten thousand one hundred eighty-five pages have been proactively so far this year, including about 600 pages relating to Occupy Wall Street records, and about 600 relating to the Jones Act waivers.

I've talked a little bit about FOIAXpress, which is, hopefully, going to be an enterprise-wide solution

1 for processing FOIA throughout the Department of
2 Homeland Security. As you know, as it currently
3 stands, each of the processing is done with several
4 different databases, different processes, limited
5 interoperability, and it's laborious, time consuming,
6 and obviously can compromise data integrity.
7 So we are working to have the FOIAXpress process
8 launched by the end of the fiscal year, and we think
9 that that is very reasonable. We'll launch it first
10 with the Privacy Office, go to headquarters, and then
11 roll it out very quickly to the components whose
12 licenses we're leveraging, including my good friends
13 from the U.S. Coast Guard. So we're looking forward to
14 having an interoperable, enterprise-wide processing
15 solution.
16 Candidly, an area of increasing concern in the
17 department is the FOIA backlog, which we've been
18 working to develop best practices to manage, but the
19 scope is quite significant. We have been meeting with
20 FOIA officers and officials from other agencies,
21 looking at technology, training, and staff development
22 ways to manage the backlog. We've also been trying to

have a surge approach to certain components who have a significant backlog.

The department's FOIA, just to remind you, was 175,000 FOIAs received last year. We look to -- we'll likely break that record this year, and we've been really trying to leverage a bunch of different opportunities.

With that said, it's still a lot of people. It's a lot of people. It's a lot of numbers, lot of things.

Turning to our last new group, which is the Privacy Oversight Committee, which is what goal number, Howard?

MR. BEALES: Five.

MS. CALLAHAN: Four. But you knew there were five goals. That was good.

(Laughter.)

MS. CALLAHAN: The fifth one is employee development. So, so privacy oversight is our fourth goal, and it's a new team created from the strategic review. But I think it's really important, and I think this committee will, hopefully, appreciate that the synergies that are created by bringing together

complementary functions are already strengthening the office's oversight role throughout the Department of Homeland Security.

Privacy compliance reviews, you're going to hear a little bit about a specific example of that when Don and Jamie testify later on. Jamie Pressman Danker also testified on how we're rolling this out about 2 years ago, and now we're going to talk about concretely how we apply it.

We've been working on privacy compliance reviews and ramping up that function basically since December, since the committee last met. Since then, the Privacy Office has released three public reviews on privacy compliance reviews, including the Einstein program, the department's use of social media for communications and outreach, and the biannual assessment of the National Operations Center publicly available Media Monitoring and Situational Awareness Initiative.

The two privacy compliance reviews conducted on social media uses are good examples of how DHS embeds full life cycle protections into systems and programs. Specifically, the PIAs for these two initiatives

1 explicitly include privacy compliance review
2 requirements in the PIAs themselves, thus enabling our
3 office to confirm that protections built into the PIA
4 process are adhered to and to identify any
5 recommendations of improvement.
6 The oversight team has an ongoing review taking
7 place of a classified multiagency information-sharing
8 environment and on DHS's participation in the ISC
9 Suspicious Activity Report Initiative.
10 In addition to looking for opportunities to build
11 privacy compliance reviews into the privacy impact
12 assessment process, we seek to spread privacy
13 compliance reviews as a best practice for the Federal
14 Government. To date, we've provided briefings to the
15 CIO Council Privacy Committee Best Practices
16 Subcommittee and during our recent privacy compliance
17 workshop, which was as I mentioned earlier.
18 And you will, of course, hear more about the PCR
19 process and the social media situational awareness
20 later on today.
21 Speaking of social media, on June 8th, the
22 department became the first department to have a

1 department-wide management directive on privacy policy
2 for operational use for social media. This is not
3 communications and outreach, which we have a privacy
4 impact assessment, and this is not on situational
5 awareness, which we have a privacy impact assessment.
6 But this is, instead, a management directive that
7 goes to each of the individuals in the department to
8 make sure that they have privacy protections in place
9 when social media is used to carry out its authorized
10 mission. The management directive and associated
11 instructions detail specific steps components must take
12 before engaging in the operational use of social media.
13 These steps include completing templates to
14 document their authority to engage in the operational
15 use, provide annual training to the department's
16 employees authorized to utilize social media, and
17 creating specific authority-based rules of behavior
18 that employees must follow while utilizing social media
19 to implement their own authorities. And I think it's a
20 really important step, and we're hoping to be real
21 leaders in this in the Federal Government.
22 Speaking of social media, on February 16th, I

1 testified before the House Committee on Homeland
2 Security Subcommittee on Counterterrorism and
3 Intelligence regarding the department's use of social
4 media. The testimony addressed the purposes and
5 appropriate privacy protections for which DHS uses
6 social media through external communications and
7 outreach via PIA, situational awareness via PIA, and
8 operational use. And that's where the management
9 directive will address that.
10 With regard to privacy incident handling or data
11 breaches, on January 30th, my office issued revised
12 privacy incident handling guidance, the PIHG, the
13 infamous PIHG. The revised PIHG is streamlined to
14 include more specific detailed guidance for all stages
15 of privacy incident handling from incident reporting
16 through escalation, investigation, mitigation, and
17 notice of affected parties to closure.
18 The version contains more relevant examples and
19 accurately represents the incident handling process as
20 it exists today. In January, the Oversight Office
21 hosted two privacy incident handling meetings with
22 component Privacy Officers, points of contacts, and

1 security operations staff. And in addition, we plan to
2 conduct outreach on privacy incidents and how to
3 leverage best practices.
4 As you know, one element of my authority that's
5 fairly unique among Privacy Officers is the authority
6 to conduct investigations. The 9/11 Commission Act
7 explicitly expanded my responsibilities to have
8 investigatory authority, the power to issue subpoenas -
9 - so watch out -- the ability to conduct regular
10 reviews of privacy implementation, and greater
11 coordination with the Inspector General.
12 Pursuant to this authority, since December, the
13 oversight team conducted two investigations that led to
14 findings of noncompliance with DHS policy. One of
15 these investigations involved a component's use of
16 social media, speaking of social media, for operational
17 use without the appropriate oversight and protections
18 for collecting and using PII.
19 Based on these findings, the oversight team
20 developed the management directive that I just
21 mentioned to make sure that the entire department
22 complies with the same standards.

1 The second investigation was prompted by a
2 referral from the DHS Office of Inspector General, and
3 the purpose of the investigation was to determine
4 whether the DHS component's information-sharing pilot
5 with an external agency was in compliance with DHS
6 policy and the Privacy Act. The investigation resulted
7 in a statement of conclusions drawn from the
8 investigations and steps to take to ensure that any
9 information sharing is implemented in a privacy
10 protective way.
11 As you can hear, the privacy oversight team,
12 although very new, is certainly very active. And so,
13 we're looking forward to the team to continue to
14 coalesce and that we're going to develop a set of
15 standard operating procedures for the oversight team as
16 part of the strategic plan and the rollout of that.
17 So, with that said, Madam Chairman, I have one
18 final note, which is this is my final DPIAC. I am --
19 after 3 1/2 years, 12 DPIACs, and 3 new committee
20 members -- departing the department as of July 31st.
21 The good news is I've got to testify on my last
22 day, as I mentioned. That's my parting gift to the

Congress. And it's also time because the office move is scheduled for August 1st. So I don't want to have to pack and unpack twice is really what it boils down to.

But, no, it's time. As you can hear, the department and the office is in a great place. The strategic plan is in a great place. We're really in a wonderful opportunity. And so, with that, my report concludes.

MS. SOTTO: Well, with that last bit, let me just say it's been a deep, deep pleasure to serve with you and for you, and we wish you enormous luck. Don't do that.

We wish you enormous luck in your new career, and you'll let us know where that is. And boy, it's going to be tough without you.

Thank you.

MS. CALLAHAN: Thank you.

(Applause.)

MS. SOTTO: You know, I will comment before turning to questions. The luxury of having privacy oversight is not something that we should take for

1 granted. I just spent the last week in Serbia,
2 advising the data protection commissioner there. I
3 can't tell you how many years they are away from
4 oversight because they don't have any of the programs,
5 of course, to support even a vaguely effective program.
6 So oversight comes much later. That is, it really
7 behooves us not to take that for granted. So thank you
8 for doing that and for really putting in place an
9 incredibly effective, well-oiled machine.
10 MS. CALLAHAN: Thanks. Thank you.
11 The oversight, I really think it is in the
12 evolutionary stage. It kind of goes through that whole
13 process, right? Policy, advocacy, compliance, and we
14 end with the oversight to make sure as part of the
15 information governance, it's all part of the life
16 cycle.
17 And I think it's really -- it's a nice combination
18 to have the privacy compliance reviews that you're
19 going to hear about be merged with the investigations,
20 as well as the incidents, right? Because it's, okay,
21 have we done what we said we did? Have we met the
22 promises we've said?

If we haven't, how do we mitigate that? How do we ameliorate that? How do we leverage it and prove it and have best practices going forward?

And so, it's a great team. It's a small team. They're mini, but mighty, I believe is what Martha calls them. But I think it is kind of a maturation of the concept and, actually, the department's acceptance of privacy as part of the whole process.

So I'm excited about it. It will be fun to watch that develop.

MS. SOTTO: Thank you.

Joanne?

MS. MCNABB: It would be -- okay, press something?

MS. CALLAHAN: Click it.

MS. MCNABB: It's all changed since this new little dealie got added. Is that it?

MS. SOTTO: It's near the number. Go down to the bottom.

MS. MCNABB: Now? Before I ask my question, which is very mundane, Mary Ellen, I've been on this committee since the beginning, and I've seen the Privacy Officers come and go. And --

MS. CALLAHAN: There have only been two others.

(Laughter.)

MS. MCNABB: I've seen them all.

MS. CALLAHAN: Right. Four in total, three official.

MS. MCNABB: So, yes. And I think what's characterized your regime has been a real deftness in blending the keeping the bureaucratic processes, the stream of reports thing that have to be done, seriously keeping that going and at the same time doing some really groundbreaking work on cutting issues, on emerging, developing issues, and really building on some of your stronger -- some of the stronger of your predecessors, on their involvement and the meat of it. You've really bitten off more of that.

I'm getting a bit of a metaphor here. But I think you've done a lot to be proud of.

MS. CALLAHAN: Oh, thank you.

MS. MCNABB: So thank you very much.

And my question is --

MS. CALLAHAN: Yes.

MS. MCNABB: I think I've asked questions like

this before and somehow maybe I just don't follow up on them. About this new online training, would it be possible for us to have access to that in some way? I know it's probably on the intranet, but can we get it on a CD or something?

MS. CALLAHAN: We can look into you guys getting access to it. It is not available on the DHS public Web site.

MS. MCNABB: Right.

MS. CALLAHAN: It is kind of a practitioner's goal, but we can look to see if we could --

MS. MCNABB: Through maybe HSIN --

(Laughter.)

MS. CALLAHAN: Okay. We can talk about HSIN offline. But it is, yes, we can see if we can get the committee members a DVD for it.

MS. MCNABB: I think it would be very useful. I know that I and I assume other people maybe in their organizations are wrestling with improving and developing a better version of training.

MS. CALLAHAN: It's hard. You've got to kind of take the balance of you want to make sure you get the

1 content there. You want to make sure you hold their
2 attention. I see Privacy Officers nodding as I'm
3 talking about this. Hold their attention, but make it
4 relevant to them, right?
5 They don't want to talk about such and such
6 exemption of the Privacy Act. They want to know, okay,
7 what do I do when I have an incident? What do I do
8 when I deal with ordinary course information, and so
9 on? And that's what we've tried to do and make it very
10 practical.
11 So the idea here is to have this kind of core
12 elements because the department is required to train
13 all of its employees and its contractors. And if you
14 look at my quarterly reports, the numbers are really --
15 there are five digits every quarter in terms of
16 training.
17 But we're going to give this core training, kind
18 of what do I need to know, meat and potatoes stuff.
19 And then kind of the idea is to then to do concentric
20 circles.
21 So, okay, so if we're talking about specific types
22 of training for law enforcement, what should they know

that's different from or more in depth than the meat and potatoes overview training? And kind of go out like that and work with the components because the component Privacy Officers, of course, know the responsibilities of their staff much more than we do and to try to help tailor it. But again, leverage it so we don't have 11 different trainings for 11 different Privacy Officers within the department.

So this is a first stage, but we're trying to help build it.

MS. MCNABB: And to support my request, I provided the training that we prepared to Becky in developing this.

MS. CALLAHAN: Duly noted, Ms. McNabb. Duly noted.

MS. SOTTO: Barry Steinhardt?

MR. STEINHARDT: Thank you.

Like Joanne, I have a question. But first, I want to offer my thanks to Mary Ellen for her extraordinary service. She mentioned very quickly something that I think is an important innovation, which is that she meets periodically, I guess quarterly, with the privacy

1 advocacy community.
2 I know those meetings are not always pleasant for
3 you, Mary Ellen.
4 MS. CALLAHAN: Actually, they're fine. That's
5 okay. Thank you for thinking that they aren't
6 pleasant. They're not bad. I have worse internal
7 meetings, Barry.
8 (Laughter.)
9 MR. STEINHARDT: I don't really want to be in
10 those. I know that meetings can sometimes surface
11 differing points of view, but I think they've been
12 extraordinarily important in allowing the advocacy
13 community -- and here I'll speak for the advocacy
14 community, although some on this committee may want to
15 offer another point of view. But I think they've been
16 extraordinarily important in allowing for free flow of
17 exchange of information between the department and the
18 advocacy community.
19 We've recently had one matter that I'm going to
20 ask about a separate matter. We've recently had one
21 matter that we had an opportunity to straighten out
22 before it became controversy. I think that's the sort

of important outcome of those meetings.

So my question is this. Can you offer us, offer the committee any sort of general information about this matter? The Attorney General has issued a directive on behalf of the President, I guess, requiring that component agencies which have personal information related to possible terrorists or who are suspected of terrorism must give that information to the National Counterterrorism Center, to oversimplify it here.

And I know that DHS has a lot of such information, and I'm just wondering what -- if you can talk about what the plans are of the department to comply with that directive and what the process is for deciding what information will be given and what for?

MS. CALLAHAN: Sure. No, I'm happy to do that. I want to do a little bit of stage setting because I know that was -- Barry spent some time paying attention to this. But just for the awareness of all the committee members.

The Attorney General is required under the Executive Order 12333, also known as 12-triple-3, to

1 approve the guidelines for information sharing for each
2 of the intelligence community agencies. So they're
3 called AG guidelines. So they're guidelines that he
4 approves in his capacity as the chief lawyer for the
5 Federal Government. Each, as I said, intelligence
6 community has these AG guidelines for handling of
7 information.
8 In March of this year, the National
9 Counterterrorism Center, which I'll define in a sec,
10 had new Attorney General guidelines that do not require
11 the sharing of information, but instead allow the
12 sharing of federally collected information that resides
13 in Federal agencies if that information is reasonably
14 believed to contain terrorism information.
15 There is not a percentage associated with that.
16 There is not an adjective associated with that. But if
17 the database itself is reasonably believed to contain
18 terrorism information.
19 The National Counterterrorism Center is an
20 organization that was stood up post 9/11 to do what?
21 To connect the dots, right? Right, we always heard
22 9/11, they didn't connect the dots. So NCTC is a

1 relatively new entity that was designed to connect the
2 dots. It is also allowed to collect information on
3 U.S. citizens, unlike some of the other agencies, and
4 I'll stop there in my description of NCTC.
5 So the NCTC has its guidelines were approved by --
6 NCTC's guidelines were approved by the Attorney General
7 to allow information sharing, and the information
8 sharing can take place in three different ways. One
9 is, "Hey, what do you know about Chris Pierson? Here's
10 the information on Chris Pierson." Right? That's a
11 pretty straightforward information-sharing request. We
12 think Chris Pierson is a terrorist, so could you give
13 us the information?
14 NCTC's authority and information to hold are for
15 any known or suspected terrorist or people with
16 terrorist ties. So if they ask for Chris Pierson's
17 information, that's pretty straightforward.
18 The other option is, "Hey, can I have access to
19 your database and search for people like Chris Pierson
20 if I have a reasonable predicate?" And NCTC has very
21 strict standards about what's a reasonable predicate to
22 be able to find it and so on.

And then the third track of this type of information sharing approved by the Attorney General in March is, essentially, I don't know who Chris Pierson is. I don't know who he is, but I have reason to be believe that he has certain indications, certainly characteristics. And if I search for it, then I'm giving away some of my classified information that you, DHS, actually aren't authorized to see.

So, or I'm not even sure I know how to search for it, but what I do know I can do is bump up my data against your data to try to find people with immutable characteristics like Chris Pierson. And that in short-term parlance is bulk sharing.

And so, all three of those tracks have been approved by the Attorney General for the National Counterterrorism Center for Federal databases that are reasonably believed to contain terrorism information.

The Attorney General has also approved that the National Counterterrorism -- so, again, NCTC is authorized to hold information on known or suspected terrorists, KSTs, because I had to give another acronym to you guys. But they also can temporarily hold

1 information on U.S. citizens while trying to determine
2 whether or not they are a KST.
3 So the Attorney General has approved that the
4 temporary retention of information on U.S. persons can
5 go up to 5 years in order to determine whether or not
6 they are a known or suspected terrorist. That
7 timeframe is an increase from 180 days, which was the
8 previous Attorney General guidelines from 2008 for
9 NCTC.
10 That's the basic framework of the NCTC guidelines.
11 They are available online. I believe in Charlie
12 Savage's article on March 22nd, they are linked. I
13 don't believe that NCTC has released them. They've
14 released them to the reporter, the New York Times. So
15 that's a way you can look at them.
16 Let me answer the question with regard as the
17 Privacy Officer, the Department of Homeland Security
18 Privacy Officer. We, if you may recall last year, the
19 Privacy Office updated five privacy impact assessments,
20 which said we're going to be sharing information with
21 the National Counterterrorism Center, and the National
22 Counterterrorism Center will be able to hold that

1 information temporarily for up to 180 days.
2 But what we did is we built in a series of
3 auditing and oversight controls. We have quarterly
4 meetings with them and go and see how the information
5 is being used. Are they abiding by the terms of the
6 memorandum of understanding that we have with NCTC?
7 What have they found?
8 Have they, for example, shared it back with the
9 Department of Homeland Security so that we can
10 implement? If you know somebody is a KST and you know
11 they're on a plane today, it would be good for us to
12 know that, right? You know, that sort of thing and
13 making sure that the information flow goes both ways.
14 That process actually in terms of, again, in terms
15 of reviewing the standards, having the Privacy Office
16 and the Civil Rights and Civil Liberties Office there
17 together looking at these issues has been, by and
18 large, successful.
19 We, therefore, worked throughout the department to
20 try to have an articulable approach to dealing with
21 kind of a blanket, blank check, so to speak. And the
22 department is in the process of finalizing a systematic

1 approach that looks at several different factors of its
2 databases. And as you said, we have a lot of
3 databases. And candidly, probably almost every
4 database would meet the definition within the
5 reasonably believed to contain terrorism information.
6 And so, we've done a variety of different factors,
7 not fully thought out, but just to kind of talk through
8 it. One is good guy data versus bad guy data. Is it
9 data that's collected in the ordinary course of
10 business as you interact with the Federal Government?
11 If so, maybe consider a shorter retention period.
12 Does it have a lot of U.S. persons information in
13 it, or is it primarily a non-U.S. person information?
14 Again, those could be factors.
15 Are there data restrictions associated with the
16 database writ large? Does it have a short retention
17 period on behalf of the Department of Homeland
18 Security? If so, again, how do we apply it?
19 What are the other factors that we want to look
20 at? Is it something, again, you're crossing a border,
21 or are you petitioning DHS in order to do such and such
22 or some sort of element? So if you're making a

1 proactive statement, maybe we have a little bit longer
2 time period.
3 So to try to have a theory so that we don't have
4 to every time we're asked for data, we don't have to
5 say, "Oh, God, what number do we think for this
6 database? What do we think of that database?" So
7 we're trying to frame this in a repeatable process and
8 a theory that takes into consideration the National
9 Counterterrorism's need and desire to have information
10 in a bulk capacity to do basically big data type of
11 comparisons while also protecting our relationship with
12 the U.S. public.
13 So we're working on that, and that's what we're
14 trying to finalize. And just to be clear, we have not
15 done new MOUs with NCTC. When we do the new MOUs, if
16 the data retention changes or any of the other handling
17 changes, we will update the PIAs.
18 And the databases that we already have MOUs with
19 NCTC are SEVIS data, which is student visa information
20 data. ESTA data -- so that doesn't have a lot of U.S.
21 person information. ESTA data, which is the electronic
22 information that's provided by visa waiver country

program, recipients who are coming here on a short-term basis. Also, it has no U.S. person information, or shouldn't.

ADIS data, which is arrival and departure information for non-U.S. citizens. So non-U.S., so visitors as well as legal permanent residents.

RAPS data, which is refugee and asylee data for people who are in the United States, but applying for refugee benefits. And APIS data, which is airline manifests for all inbound and outbound flights to and from the United States. Oh, sorry. To the United States, not from. Just to the United States.

MS. SOTTO: Okay. I'm going to move us along. Sticking with the agenda, but I hope you'll hang around later.

MS. CALLAHAN: Sure. Sure, sure.

MS. SOTTO: So we can all give you the big hugs that you so richly deserve. Thank you very much, Mary Ellen.

MS. CALLAHAN: Sure.

(Applause.)

MS. SOTTO: Don Triner and Jamie Danker, please.

Thank you very much for joining us. While they're getting seated, I'll introduce our next witnesses.

As Mary Ellen mentioned, we are delighted to welcome Don Triner and apologize for keeping you hanging around last time. And we're delighted to have you this time around.

Mr. Triner is the Director of the Operations Coordination Division in the DHS Office of Operations, Coordination, and Planning. And Jamie Danker is the Associate Director of Compliance in the DHS Privacy Office.

Mr. Triner's responsibilities include the National Operations Center, as well as the DHS Crisis Action Process, which is a 24/7 operations information flow and assessment for the Secretary, White House, and all homeland security partners. Mr. Triner also provides strategic leadership to the DHS Current Operations and Future Operations Branches. And before joining, he served as a captain in the U.S. Coast Guard, and is that why I see your cronies here?

(Laughter.)

MS. SOTTO: Ms. Danker is responsible for

1 conducting privacy compliance reviews for the DHS
2 Privacy Office. Before joining DHS, Ms. Danker spent 6
3 years at the U.S. Government Accountability Office,
4 where she conducted Government-wide and agency-specific
5 reviews involving privacy issues.
6 Welcome to you both. Mr. Triner, please proceed.
7 MR. TRINER: Thanks.
8 Jamie, you want to go first?
9 MS. DANKER: Sure. I'm just going to try to set
10 the stage a little bit before we get into the details
11 of the NOC media monitoring initiative.
12 So almost 2 years ago, I came before the committee
13 and talked about establishing a privacy compliance
14 review process. And now we're almost 2 years in, and
15 with Mary Ellen's support, we've published 9 public
16 reports on the results of privacy compliance reviews.
17 Many of them are related to this NOC media monitoring
18 initiative.
19 But just want to put the PCR in context. We have
20 our privacy compliance life cycle, which sometimes
21 begins with the privacy threshold analysis, which can
22 lead to a privacy impact assessment, a system of

1 records notice, and the newer thing is the privacy
2 compliance review. In the case of the NOC media
3 monitoring initiative, we built the requirement for the
4 PCR directly in the PIA.
5 So the initial interaction with Don's shop began
6 in 2010, and it was begun as a series of pilots. And
7 there were privacy impact assessments performed for
8 each, each of the pilots, followed by privacy
9 compliance review of the pilots.
10 Each of the PIAs are a FIPPs-based analysis of the
11 program. Again, transparency through publication of
12 the PIAs, data minimization initially in the pilot was
13 not allowed to collect any PII whatsoever. These
14 limitations were in place, only used for situational
15 awareness and establishing a common operating picture,
16 and data quality and integrity, redacting any PIA
17 outside of discrete categories, and a very short
18 retention period, which I believe is 5 years, and then
19 auditing accountability is the PCR process.
20 So after the series of pilots and positive
21 assessments of the privacy compliance reviews, there
22 were some updates made to the initiative that permitted

1 limited PII collection on seven narrow categories of
2 individuals. And when I say PII, I'm not talking about
3 a whole dossier of information on individuals. It's
4 just full name, affiliation, position title, and
5 publicly available user ID.
6 So I'll get into the most recent results of our
7 privacy compliance review. But first, you're probably
8 wondering what is this NOC media monitoring initiative?
9 And so, I'll just hand it over to Don.
10 MR. TRINER: Thanks, Jamie.
11 Madam Chair, thank you very much for inviting me
12 here today.
13 Can everyone hear me all right? Okay, super.
14 So, really, I think everyone has the slides on
15 their deck. If not, they are behind you. I apologize
16 for that there. But this goes all the way back to 2005
17 as part of the lessons learned after Katrina. One of
18 the things that we were criticized in the department at
19 that point in time, we only reported on things that
20 were actually confirmed by a Federal source.
21 So if things were in the TV or on the media and we
22 didn't actually report on those, even though you may be

able to see them right there in your own living room, until someone actually told us. So one of the major criticisms we had was why aren't you using what's available in the media as part of that responsibility you have in statute, which the national operation has, to provide situational awareness and the common operating picture to all of the homeland security enterprise -- Federal, State, local, tribal, territorial, private sector -- all of our partners and make sure that we know what's going on.

So we brought on this initiative to try to use what was available to get the information from the media. It's sort of like an early warning, like a canary in a coal mine of what's going on. Then we can further take action.

Because we know from our own research it takes about 2 hours from the time something happens until one of our Federal partners or State partners actually tell us something happened. And we find that by using the media, we actually can get a leg up on what's going on.

So, first of all, in case you don't know, the National Operations Center is actually five elements in

three locations. So it includes not only the Nebraska Avenue complex, which has the National Operations Center watch and our link to the intelligence community through watch and warnings, but it also includes the National Infrastructure Coordinating Center, which is our link to the private sector, as well as the National Response Coordination Center, which is FEMA's link to all of the emergency operations centers in all of our States and territories, as well as our planning element, which really helps provide rapid crisis planning in time of an event.

So that's really the requirement of the NOC is to be that hub for information into and out of the DHS for all our homeland security partners. This is one small piece of what we do every day.

And anytime something is not clear or I use an acronym or anything else, just please raise your hand or ask me a question, I'll be happy to answer that.

So, again, the key here and why I like sitting with Jamie is that we really work very, very closely with our privacy partners. We really are very, very lucky to have them to help us really be able to work

through issues to make sure that we don't make mistakes because we really want to do this the right way and really avoid misperceptions.

We weren't totally successful in that endeavor, but that was really our goal there. And we really wanted to make sure that we worked with them. And to explain what we're trying to do, they've really been very, very helpful to make sure that we understood the law and to make sure that we comply with all of our privacy responsibilities from early in the start on there.

So, really, the focus was on not who is saying it, but what's being said. What's happening? What's burning? What's exploding? What's being fired upon? What's dying? Those type of questions, not really worried about who's saying it. That's really just the indication that something is going on.

We can then use our Federal resources, our State resources to find out what's going on. It's just an early indication that something is going on and what it might be. As most folks know, most first reports are false, but something is going on in there.

1 So we find that 94 percent of the events that we
2 report on, we first find out about through the media,
3 through both traditional and what we call new media or
4 social media. And really focused on things that are
5 already commercially available to the public or that
6 are available for a subscription price.
7 We don't have any -- we haven't built any special
8 tools or any special search capacities. We're really
9 using what's already available on there. And then we
10 distribute to our homeland security partners, primarily
11 Federal -- we do have some State and some private
12 sector partners in there -- based strictly on their
13 request on there.
14 We produce information about every 30 minutes
15 about something going on in the United States that
16 comes into the homeland security mission. So a great
17 amount of information reporting that we're doing on any
18 given day.
19 We're very, very proud of what we've done there
20 working with privacy because this is really not an
21 intelligence function. This is really not a law
22 enforcement function. This is really about complying

with our privacy impact assessment and our system of records notice to really get that information about what's going on.

We learned in the process that it was helpful sometimes to be able to use names. And what I always get is, actually, the privacy rules we applied first were so strict we couldn't even talk about that person who lives at 1600 Pennsylvania Avenue because that was the President and that was personally identifiable information.

So we actually put in reports "unknown Federal official" or -- and it'd be like, "Don, come on. Really? You can't say the President?" Or the news, the name of a news reporter that may have certain credibility to the report if one person is reporting that versus another. And it would really get clunky when we had to write around some of those things.

Or if we had a very famous criminal who had been maybe killed in a gunfight or a known -- when we actually took down bin Laden. In the early partials, we couldn't even talk about that by name. We'd have to say "some famously known terrorist" in there. So

that's the level that we tried to -- but it really brought our credibility into question with some of our less privacy-savvy users about why we were doing that.

Is this some sort of game you guys are playing with us to make us click on the links and look at stuff? And it wasn't. So we get some very limited exemptions for us to actually collect personally identified information and really is one you would expect. You put something online because you're being attacked in your house. You saw people walk into a bank with guns. You saw bad people doing things.

You'd want us and expect us to be able to tell local law enforcement that this person has done this and then investigate that. So that's the in extremis type situation. You're watching bad people do bad things right now. Very, very rare, but I'll give you an example of one we actually had during Haiti.

During the Haiti earthquake, which is one of our pilots, we actually had a privacy impact assessment. We were operating under very strict rules there, but we actually got a notice through new media that "I'm an American diplomat, and I'm trapped in the rubble in

Port-au-Prince."

So we went to the State Department and told the State Department, "Hey, we have this information." The State Department then went down range to Port-au-Prince, and they had accounted for all of their diplomats. So, in fact, that wasn't true.

There were no reports issued. Nothing was recorded. There was no database entry.

About 19 days later, we got another -- we picked up again on social media, I think it was on Twitter, that "I hear tapping in the rubble by this hotel." We, once again, were able to get in touch with the State Department through State ops into the consulate, into the response team. And lo and behold, they actually found someone in the rubble in Haiti, based on that exemption in there.

So, remember, that was actually the very last person they found, set all kind of records like you never had anyone in the rubble this long in their whole life. That was an example of that type up there.

The other thing we try to be very, very careful of is quite often now, especially in new media, reporters

1 in particular have their names as part of their link or
2 part of their post or entry. So we strip that
3 information out, and we stay away from that as well.
4 That's really been a challenge for us.
5 And again, we're not generating any new
6 information. We're just packaging that which is
7 already available publicly for folks in there. So the
8 redress would be back to the source document, which
9 would be the reporting agency and not on the National
10 Operations Center in there.
11 We're not interacting directly with the media --
12 with the public either. So, in other words, we're not
13 going back when someone posts something on the Internet
14 or puts information on, we're not -- there's no back
15 and forth. There's only observation. There's only
16 review of that.
17 We're not asking them for information, asking them
18 for more information, asking them to do anything that
19 they aren't already doing other than reporting. So
20 we've been very, very successful in, first of all,
21 training all of our ops folks in how to handle
22 personally identifiable information to comply with all

1 of our privacy responsibilities, to make sure that they
2 understand. This includes both classroom, study aids,
3 as well as on-the-job training and review of that.
4 We have a very rigorous review process. I think
5 through this we've generated about 21,000 items of
6 interest through NOC media monitoring, and we have had
7 17 inadvertent releases of PII. So that's 99.9992
8 percent success rate. Not good enough. We want to be
9 correct all the time. So we've instituted some more
10 reviews on this so that we're really down to the last 2
11 months we haven't had a single inadvertent release of
12 PII.
13 And just so you get a sense, it isn't like -- this
14 isn't like the person that's emailing had their name in
15 that. One of it was we thought the person had been a
16 known narco-terrorist in Mexico that was killed, and in
17 fact, he wasn't killed. So those are some of the
18 examples of some of the PII releases that we made
19 inadvertently and then purged those from our system as
20 soon as we found those.
21 We've gone from a 6-month review cycle to a month
22 review cycle to now every 2 weeks. We look at all the

1 data, all the reports we have issued to make sure we're
2 in compliance with the PIA that oversees that.
3 Next slide for me.
4 And then really, so I want to make sure you know
5 this is really about the -- so this is not a sum total
6 report. This is just an early information source to us
7 of something is going on. So we're going to be using
8 other information sources we have as we help give
9 senior leaders an early warning of the decisions they
10 may have to make, give some of our partners early
11 warning of things that may be going on.
12 Again, we're looking at things that are exploding
13 or burning, our traffic being impacted, hospitals being
14 out of power. Those type of events that are going on.
15 And then really leverage our other data sources to
16 make sure we get a full story of what's going on. But
17 this is that early indication of how we're going to use
18 that and how we're going to work on that.
19 And then we also look at -- every report we do, we
20 then cross-check it with all of our folks to make sure,
21 hey, why did you report on this? What does it have to
22 do? Is Johnny always reporting on explosions? Is Jane

1 always reporting on traffic jams?
2 So we really look across the whole homeland
3 security enterprise to make sure that the information
4 that we're thinking is important to our homeland
5 security enterprise actually is from the whole dataset
6 of things that we want to see and not just one thing
7 that they're focusing on. To make sure they really are
8 doing the job of providing that situational awareness
9 across all of our mission areas.
10 The last thing that we wanted to make sure was
11 that we had, since our analysts have unfettered access
12 to the Internet, just like you would at home, we wanted
13 to make sure we knew where they were going. So we have
14 a very rigorous audit program that tracks exactly where
15 they've gone, where their clicks have taken them, and
16 we monitor that against known blacklists of bad sites
17 that you wouldn't want your employees on, whether
18 that's gambling or other type of things that are on
19 there, to make sure that we know exactly and we can say
20 exactly where they've been.
21 And we're also adding in a feature, an auto
22 feature that if someone actually types in a search term

that we actually know any searches they did against the report database that we have. But again, it's free of PII, but we just want to make sure that we know exactly and can show and prove exactly that we are in compliance with all of the requirements that we have on us because it's very, very important to us to make sure that we're doing that.

So, really, that sort of ends my prepared comments on what we do with the National Operations Center. I'll be happy to answer your questions after Jamie or now, as the case may be.

MS. DANKER: Does anybody want to ask any clarifying questions about the capabilities before I talk about the compliance review?

MS. MCNABB: I have one.

MR. TRINER: Sure, ma'am.

MS. MCNABB: So you said that if you inadvertently have pulled in PII that you dump it right away?

MR. TRINER: Yes. As soon as we realize we have it.

MS. MCNABB: Yes. So then, and then I thought you said that later on that you might -- one of the things

1 you might be looking at in determining the potential
2 sort of accuracy is has Johnny or Jane been sending
3 this kind of thing. How do you know who the sender is?
4 MR. TRINER: I'm talking about my own analyst, my
5 own analyst folks on one thread. Not --
6 MS. MCNABB: Oh, okay. Your analysts. Okay, got
7 it.
8 MR. TRINER: -- what citizen Jane or citizen
9 Johnny.
10 MS. MCNABB: Got it. Thank you.
11 MR. TRINER: Yes, sir?
12 MR. NOJEIM: You collect PII on --
13 (Pause.)
14 MR. NOJEIM: You collect PII on reporters, right?
15 People who are reporting incidents, no?
16 MR. TRINER: Well, we are authorized under
17 circumstances where we think it would lend credibility
18 to have that reporter's name in the report.
19 MR. NOJEIM: If I'm a blogger and I am blogging
20 about some incident, would you collect my name?
21 MR. TRINER: If your name lent credibility to the
22 report, yes. Otherwise, no.

1 MR. NOJEIM: So if I am a reliable blogger, yes?
2 MR. TRINER: We don't collect information on
3 reliability on the blogger. So we wouldn't know that.
4 MR. NOJEIM: Then how would you know whether to
5 collect my name?
6 MR. TRINER: If you were on television. I don't
7 want to collect your name. It would only be using your
8 name in the reporting if it lent credibility. I can
9 think of no circumstance would the reporter's name from
10 a blog that we have used.
11 MR. NOJEIM: Let me just summarize my concern.
12 MR. TRINER: Sure.
13 MR. NOJEIM: It is that when you collect from
14 social media information that a person puts out there,
15 there is a risk that you will chill that person from
16 continuing to put that information out there. And I
17 think that's one of the reasons why you have strict
18 rules about not collecting PII.
19 The PII of the speaker as well as of the victim,
20 those are all important considerations. So I guess my
21 question, my concern is when the speaker is a person
22 who is not, they're not a professional journalist --

they're just doing this as their hobby -- how do you decide whether their name gets collected or not?

MR. TRINER: They would not be.

MS. DANKER: I would also refer you to the privacy compliance review report. We actually did a breakdown for a 6-month period for all the reports that contained PII within the 7 permissible categories, what that breakout was. And the copy I have in front of me is in black and white, but I believe that that reporter's category was only 2 percent.

Two percent of all the reports that contained PII, contained PII on the category called "anchors, newscasters, or on-scene reporters who are known or identified as reporters."

MR. NOJEIM: So these -- I won't belabor the point. I think you get my concern.

MR. TRINER: I understand your concern. Just so in the last 2 months, there were almost 3,000 items of interest. In only two cases did we use that where it lent credibility, and it was people that you would recognize the face and the name that it provides some sort of credibility to the report.

1 So it's a very, very limited case we try to do
2 that. The other thing we try to protect and sometimes,
3 again, their information shows up in their link to
4 their story or their report in there. But again, in
5 just 2 out of the last 3,000 we used that exemption,
6 and in no cases would these be things that -- it really
7 has to lend credibility.
8 So we're really on the point to make sure that
9 it's not really -- it's the exception, not the rule.
10 And we're not really collecting on them. It's really
11 part of the story.
12 MR. NOJEIM: One other question, if I may?
13 MR. TRINER: Sure.
14 MR. NOJEIM: So that the PIA says Federal law
15 requires the NOC, that's you, obviously, to provide
16 situational awareness and establish a common operating
17 picture for the entire Federal Government and for
18 State, local, and tribal governments as appropriate and
19 to ensure that critical disaster-related information
20 reaches Government decision-makers.
21 To me, that suggests that social media monitoring
22 occurs regardless of whether there is a natural

1 disaster or an incident. That you're really monitoring
2 to see whether one is occurring, not just when one has
3 occurred. Is that correct?
4 MR. TRINER: I don't -- ask me the question again
5 because I'm not understanding the difference.
6 MR. NOJEIM: There is one scenario where you would
7 monitor social media because an incident has occurred.
8 MR. TRINER: Yes.
9 MR. NOJEIM: And so, you want to see what's going
10 on. You want to understand the extent of the problem,
11 what people are saying about it.
12 MR. TRINER: Yes.
13 MR. NOJEIM: There is another way to monitor,
14 which is to monitor to see whether an incident has
15 occurred. The latter requires that you monitor at all
16 times. Which is it that you're doing?
17 MR. TRINER: Both.
18 MR. NOJEIM: So you are monitoring at all times?
19 MS. CALLAHAN: Maybe I can clarify, Don?
20 MR. TRINER: Sure.
21 MS. CALLAHAN: If you don't mind. So on the slide
22 that's up there you can see is unfettered access

restricted to mission activities. So we're monitoring associated with the homeland security authorities and specific mission sets. So to the extent that we're "monitoring all the time," it's only associated with those equities that's referenced in that quote that you said, associated with activities that the NOC is required to report on.

So, to your point, yes, we may be monitoring to see if a fire happens, if an earthquake happens. But we only analyze the information and possibly collect and possibly disseminate the information if it's associated with those underlying homeland security missions.

So we have to have a situational awareness for 24/7 because we don't know when the earthquake is going to happen.

MR. NOJEIM: So as I read the PIA, at all times you're monitoring Hulu, YouTube, Flickr, Twitter, Facebook, and you're monitoring for terms like "games, facility, flu, cloud, leak, gas, burn, virus." Is that correct?

MR. TRINER: Yes.

MR. NOJEIM: Now the statutory charge reads a little differently. When I looked at the statutory charge, I thought that you might be monitoring when you're not meant to.

Here is the statutory charge, Section 515 of the Homeland Security Act, as amended. "The NOC is the principal operations center for the department and shall, one, provide situational awareness and a common operating picture for the entire Federal Government and for State, local, and tribal governments as appropriate in the event of a natural disaster, act of terrorism, or other manmade disaster."

To me, that sounds like you're supposed to be doing the monitoring when the disaster happens, not all the time. Am I misreading it? Where is the authority to monitor at all times?

MR. TRINER: The mission of the department is not just a response. It is to prevent, protect, respond, and recover. So it really is -- there are things that happen before the boom occurs, and so I mean, it's not just after it happens. You want people to be moving to respond as soon as you could know.

1 The example that Mary Ellen gave with the
2 earthquakes with the U.S. Geological Survey. We have
3 an amazing USGS survey system. So as soon as the earth
4 trembles, we get notification that's happening.
5 For most of our other mission areas, manmade and
6 natural, we don't have the same early warning system.
7 So we're really leveraging the first responders, the
8 folks on the ground to say what's going on in that
9 prevent, protect, respond, recover.
10 MR. NOJEIM: So the section that I read, isn't
11 that the statutory authority on which you rely for
12 doing social media monitoring when there is a natural
13 disaster. Is that correct?
14 MR. TRINER: I don't know the answer to that
15 question. That is the statute. We're allowed to
16 provide situational awareness, common picture to the
17 entire Federal family across all of our mission spaces,
18 not just after something happened.
19 MR. NOJEIM: But the problem is that the statutory
20 charge refers to something happening. That that's when
21 you're supposed to be providing the situational
22 awareness, and it seems like you're doing that

provision outside of that --

MS. CALLAHAN: So, Greg, Don is an operator, not a lawyer. To answer the question about situational awareness, Section 515 is one of the authorities that we did cite. That's absolutely correct. But as I said, as Don alluded, the NOC has a variety of different common operating picture opportunities that the NOC has to do.

So with regard to the life cycle and the Quadrennial Homeland Security Review, right, those are all of our different missions. We have the prevent, protect, and ensure. And so, the process is to go do it.

I want to clarify something where you go and you use the word "cloud" and all those sorts of things. The way that the system is set up and as Don described it is the only information we see are associated with those -- the words that you identified and a series of others that have been in our privacy impact assessment since June of 2010.

So we have these words out to be very clear, and what it is, it's to filter, to only see the

1 communications that may contain that word. Because it
2 may be about cloud computing, and it may also be a
3 cloudy day. A cloudy day, we don't do anything farther
4 with it.
5 If it's about cloud computing and some sort of
6 problem and that sort of thing and it's germane to the
7 different mission sets that the NOC is entitled to keep
8 situational awareness about, they may go and analyze
9 it. They may collect the information, and they may
10 summarize it into a report.
11 The reports, examples of the reports, were
12 provided at one of the advocacy meetings and then
13 attached to the most recent privacy compliance review,
14 which was published in May of 2012. But so I just
15 wanted to distinguish it's not that we look at
16 everything that has the word "cloud" in it. What we do
17 is only look at the words that are associated within
18 that that could possibly be about homeland security
19 missions.
20 So we use commercially available software that
21 narrows the search down. So we don't see the
22 extraneous stuff, and the stuff that we do see, by and

large, is not germane. But the stuff that is germane allows us to support our mission more -- better.

Hopefully, that will help clarify it a little bit.

MS. SOTTO: All right. I'm going to move this along so others can get a chance to weigh in as well.

Howard Beales?

MR. BEALES: I just -- I mean, it seems to me that a big part of the value here is this finding out 2 hours earlier, that it's 2 hours before your other systems report for this. What I want to understand is you also mentioned that most of the reports that something happened are false.

Are you putting out a lot of false reports, or are we screening those first? How are we doing that?

MR. TRINER: Sure. So most first reports are not 100 percent accurate is probably a better way to say it than totally false. So what we do is once we have information that something is occurring in a locale, first we'll notify our Federal partners, all of the Federal operations centers, "Hey, we have this report that this has just exploded. What do you have on this information?"

1 So that's the form of NOC reporting that we do in
2 that. And then if it was a specific State, we'd then
3 go through either the fusion center or the EOC to get
4 information. "Hey, are you aware of this? What do you
5 know about that?"
6 MR. BEALES: But presumably, in that process,
7 you're passing on or you end up passing on and asking
8 about at least a lot of things that didn't actually
9 happen? Nothing blew up is the answer.
10 MR. TRINER: Not usually. So there is some -- the
11 analyst there in the meanwhile is going to look at
12 something. So we're not going to run with one report
13 and run off with the report. They're going to look to
14 see once they use some of this, some of the newer
15 media, they may go to the traditional and see is it on
16 CNN? Is it on BBC? Is there other corroborating
17 information going on?
18 So it's not a rapid push-out. It's faster than we
19 would have been notified. But we really strive not to
20 put out the wrong information, lest the truth is
21 changed.
22 MR. BEALES: Do you know anything about, I mean,

how often is it accurate? How often was there really an incident?

MR. TRINER: We get very few that there aren't -- that the thing is totally false alarm.

MR. BEALES: Okay.

MS. SOTTO: Barry Steinhart?

MR. STEINHARDT: A question. You monitor not only for natural --

MS. SOTTO: Barry? You just turned yourself off, I think.

MR. STEINHARDT: You monitor not only for natural disasters, but you also have authority to monitor for manmade incidents in the form of terrorism. Can you tell me what the operational guidelines are to prevent you from monitoring lawful political activities, as opposed to criminal acts or acts of terrorism, which are, by their nature, criminal acts?

MR. TRINER: So we're talking about making sure that we're not monitoring the First Amendment rights of our citizens?

MR. STEINHARDT: Yes.

MR. TRINER: We tell them not to monitor the First

1 Amendment rights of our citizens.
2 (Laughter.)
3 MR. STEINHARDT: But how do you operationalize
4 that?
5 MR. TRINER: Sure. We give them very strict
6 guidelines on things. So even if there are First
7 Amendment activities going on, we really only would be
8 concerned that, let's say, we're blocking access to a
9 hospital or blocking access to a Federal. So that's
10 operational information. A fire station can't respond.
11 I don't really -- I'm not really overly -- I'm
12 really not going to be reporting on who it is or what
13 they're doing, just what that would be. But as far as
14 people exercising First Amendment rights, they're
15 strictly forbidding to even report on that.
16 So, I mean, and then we can monitor and see what
17 sites they've been going to, our analysts. And then we
18 can also look and see any searches they've been doing
19 on that. So that's part of the training. It's part of
20 the review.
21 I get all of the reports. Mary Ellen gets all of
22 the reports. They're read to make sure that those

activities aren't going on. And then our onsite, they're supervised by a Federal senior watch officer who has full oversight of what they're doing, the activities they're involved in.

So, as far as monitoring where they've been, seeing what they're reporting, and then reviewing what's being produced, all underlying with the PIA, the SORN, and their training, that's the things that we try to make sure that we are in full compliance with that.

MS. DANKER: And as another example, as part of the last privacy compliance review, we've reviewed all of their guidance to make sure that it was explicitly clear that monitoring a First Amendment activity is not -- prohibited. I mean, that was very clear to the analysts when we meet with them. They wouldn't think of that. They're focused on the what, not the who.

MS. SOTTO: Jeewon?

MS. KIM: I have a question that is related, to build upon the questions from my colleagues. In the last slide, it says that the data is collected using the COTS product, and then it goes through the filtering process using the custom application.

And Mary Ellen also mentioned that you use a commercially available software. Could you tell us a little bit more, to the extent that is possible, about the technology that is used to filter if you are to comply with the privacy policies and for data manipulation, for effectiveness, First Amendment rights issues, et cetera?

MR. TRINER: Sure. Two different -- you asked me two different questions. So this is strictly about watching where the analysts are going. So that's what this is talking about, making sure that as you do your job and you click on different sites, you get this information.

We know precisely where you've been, and we check where you've been against the known blacklist and the known places that you shouldn't be going and those type of things, you know, gambling Web sites.

The other thing, what Mary Ellen was talking about, TweetDeck is an example of a pretty relatively known, publicly available, is the different mash-up tools. Just bring a lot of stuff together to say, hey, what's the most common things being talked about right

now, and does that match against any of the pre-established words that we've used in this?

So we put in those pre-established words, and we use those tools to see what's -- is that something that we're interested in, based on our homeland security missions.

MS. KIM: I think I was going more towards the technology that is used. I mean, maybe there isn't sophisticated technology, but I guess what is the process that you use by the analyst to filter? Because there is a world of data out there.

But how do you know what is relevant, and how do you really get it down to the data that is important?

MR. TRINER: Sure. This is the important person part of the whole process in complying with the privacy rules, but also being an air-breathing, thoughtful person watching what's going on.

So we do not have any specialized tools when it comes to the use of traditional or social media on there. We have some subscription services that you're familiar with. CNN provides subscription services. Different news services on the Internet have those.

Mash-up tools that are available that it sort of synthesizes, brings together a whole bunch of information that's presently on the Web right now that's there. Again, all framed around not just broad in the wild west, but all locked in and framed around our privacy impact assessment and the known search terms and the known -- and the traditional news-type Web sites that we're going to, to confirm that.

But we're not -- so we have no specialized -- we haven't built any tool. We're not in partner with any member of the intelligence community in what we're doing. It's really what's available to -- would be available to you.

MS. CALLAHAN: So if you want, the answer is TweetDeck. That's the software we use.

MR. TRINER: There's a number of those. That's an example.

MS. CALLAHAN: There's a number of them. That's just the main one that kind of helps use the certain terms to filter it out.

MR. TRINER: That's the one we use the most.

MS. CALLAHAN: Yes. So I don't mean to promote

TweetDeck, but I know you were asking for the name.

MR. TRINER: That's why I try to stay away from talking about.

MS. CALLAHAN: You did say it. You said TweetDeck, and she was like, "Excuse me?"

But that's the primary tool, but there are other ones, as he said, to try to help filter to get to just the universe that we should be addressing.

MS. SOTTO: All right. Greg, why don't we give you the last word, and then I'd like to turn to you, Ms. Danker.

MR. NOJEIM: There was a slide that you showed the bottom line --

MS. SOTTO: Mic, Greg.

MR. NOJEIM: The bottom line on one of the slides you showed said that redress occurs through the public media site. Could you explain what that means?

MR. TRINER: Sure. This is part of the privacy impact assessment where we're required to provide that information publicly as far as what's the redress process that's allowed there. And the privacy impact assessment really points out, we're not gathering this

1 information from classified sources. We're not
2 gathering -- we're gathering this from the source.
3 So this is what CNN is saying. So that's not --
4 if the individual citizen says, "I never did that, that
5 wasn't me," it's really back to the source of that
6 report, not us.
7 MR. NOJEIM: I see. I see.
8 MR. TRINER: That's what I was trying to get to.
9 I answered one right.
10 MS. SOTTO: Okay. Ms. Danker, why don't you go
11 ahead, please?
12 MS. DANKER: Okay. So just to recap, the
13 initiative began in early 2010 as a series of pilots,
14 and then there was a privacy compliance review
15 conducted on the pilots. At that point, there was no
16 PII collection permitted at all.
17 There was a positive assessment and then
18 compliance got together with the program, and they
19 talked about how there are circumstances where having
20 limited PII included in the reports lends credibility
21 to those reports. And so, for transparency, we updated
22 the PIA to allow limited PII collection on seven

1 discrete categories of individuals, those four data
2 elements I mentioned earlier.
3 And as part of that PIA, we built in biannual
4 privacy compliance reviews. So the most recent we
5 started in March of 2012, and we published it in May
6 2012. And all of the privacy compliance reviews have
7 been available on this initiative, and I would highly
8 encourage everyone on this committee to read the most
9 recent report because I think it answers a lot of the
10 questions that are being asked today, including what
11 exactly these reports are.
12 We did a random sample of I think we picked 4 days
13 at random of all the reports that were distributed out
14 during that time, and I think it will give you a good
15 sense of what we're actually talking about here.
16 So for those of you who are new to the committee,
17 I just want to spend a couple of minutes talking about
18 what privacy compliance reviews are. Mary Ellen talked
19 about the creation of the new privacy oversight team,
20 which I joined. Privacy compliance reviews were
21 previously in the compliance group. It is part of the
22 compliance life cycle, but it is an oversight aspect.

1 But the key distinction here is privacy compliance
2 reviews are a constructive mechanism to assess
3 implementation of protections. They are different than
4 investigations. It's more we're implementing a
5 program. Let's go and see how you guys are doing.
6 Let's see how we can improve. So it's really done hand
7 in hand with the program.
8 The outcomes and benefits of the PCR are
9 recommendations to the program resulting in
10 improvements. I think every privacy compliance review
11 we've done for the NOC media monitoring initiative,
12 while we found general compliance, we've always found
13 areas for improvement.
14 Sometimes you get updates to privacy documentation
15 as the result of a review, and really one of the most
16 beneficial things are informal discussions with
17 operators about the lessons learned. They can result
18 in a formal report, as in this case, or an internal
19 report. And just generally heightened awareness by all
20 participants about privacy and also early issue
21 identification and remediation before you have the
22 Inspector General coming in and when there is really a

1 major issue. This is really to help them resolve any
2 issues early on.
3 And the basic steps of a privacy compliance
4 review, you start off with collecting and reviewing the
5 available background information, followed by
6 formulating your review objectives. And for compliance
7 reviews, one of the objectives is always to assess
8 compliance with existing privacy compliance
9 documentation.
10 Third step is notifying the program, and buy-in is
11 really, really critical. I think we're the only
12 department right now that has this kind of process in
13 place. And it really takes buy-in from the program to
14 get these built in.
15 Step four is formulating the review questions and
16 document requests. For each NOC media monitoring
17 review, we do a questionnaire and we provide that in
18 advance of the meeting. So if there are any follow-up
19 questions that need to be clarified, we can have that
20 done before.
21 And just, again, a reminder that this is a
22 constructive process. Our goal is not to say "gotcha."

1 It's you want to maintain communication with the
2 program. There really should be no surprises with the
3 types of things we're going to be asking for.
4 We conduct interviews and obtain supporting
5 documents, analyze that information, conduct
6 interviews. We try to draw preliminary conclusions,
7 and we review and confirm our findings with the
8 operators. And then if you're going to issue a public
9 product, we would let the program review that report
10 before it gets released publicly.
11 So that process applied to the NOC media
12 monitoring initiative. Our objectives were to assess
13 compliance with the 2011 PIA and the SORN. And another
14 objective that we added here, because there were
15 concerns about some of the guidance materials for the
16 initiative, was just to review them and make sure that
17 they accurately reflect the scope of the initiative.
18 So, overall, I'm just going to give you a brief
19 summary of what we found. We conducted this from -- I
20 believe it was from August 2011 through March 2012 were
21 the dates that we looked at for this biannual
22 compliance review. And basically, the questionnaire

1 questions were developed based on the requirements that
2 are contained in the PIA.
3 So we looked at collection of information. One of
4 the requirements is that they are not to actively seek
5 PII in its reporting. We found that that was the case.
6 They were not actively seeking PII.
7 And we also asked them to look at all of the
8 reports they issued for that 6-month time period and
9 then identify those reports that contained PII within
10 the 7 categories and then even do a further breakout of
11 how many reports within each category did you report
12 on? And there's a nice little pie chart in the privacy
13 compliance review that will give you a sense of the
14 most frequently used categories.
15 It's generally spokespersons from -- got it. Yes,
16 senior and U.S. Government officials who make public
17 statements or provide public updates and U.S. and
18 foreign government spokespersons who make public
19 statements or provide public updates.
20 So, overall, for that 6-month period, 20 percent
21 of the reports contained PII within the 7 permitted
22 categories. Only 5 reports contained unauthorized PII,

1 and I think that's 0.0006 percent. So pretty good
2 compliance rate there. And for those five reports,
3 there were redaction notices issued.
4 And then for use of information, they've
5 established reporting categories events consistent with
6 their statutory mandate, and the report specifically
7 will identify those 13 categories. Some of those are
8 terrorism, natural disasters, hazmat, cybersecurity,
9 transportation security, just to name a few.
10 And also our review of randomly selected reports
11 for that period reflected the variety of topics within
12 the 13 categories, and PII included within those
13 reports was always within the 7 categories. And again,
14 I would refer you to the appendix of the latest privacy
15 compliance review to get a flavor for what the reports
16 actually look like.
17 Retention of information, the PIA states that they
18 will retain all the reports distributed for a period of
19 5 years. We haven't reached 5 years yet, but one of
20 the questions we did ask was when you did find PII that
21 was inadvertently included in a report for those 5
22 instances, did you make sure to redact the reports that

1 were in your reports database? And they did, indeed,
2 do that.
3 For internal and external sharing and disclosure,
4 they have a process in place to determine the need to
5 know for report distribution. And technical access and
6 security, Don talked about their audit capability, and
7 during the reporting period, they did 14 random audits
8 and did not find any inappropriate behavior.
9 And then privacy training, this one was actually
10 pretty interesting. We actually took a look at their
11 training materials, and they're pretty comprehensive.
12 It's not a very easy test. All the analysts
13 successfully passed an annual PII certification exam.
14 So although we found them compliant, there's
15 always room for improvement, and so we identified three
16 recommendations in this report, two of which they've
17 already addressed. The last one, we will follow up
18 with when we do the next privacy compliance review.
19 The first one was related to the guidance and the
20 standard operating procedures to more accurately
21 reflect the scope and purpose of the initiative. A lot
22 to Barry's question about just clarifying that

1 monitoring First Amendment activities is not the
2 intent. It's not the intent. It was never the intent
3 of the analysts, but let's make sure that our
4 documentation is very clear to that effect.
5 Also we recommended they incorporate guidance into
6 SOPs about use of social media accounts. And the third
7 was to develop and implement a logging mechanism for
8 the reports database. That's the database where they
9 retain all the reports that were distributed for a
10 period of 5 years.
11 We wanted them to develop a log to further
12 demonstrate that they're not maintaining a database of
13 reports on individuals. So if they actually developed
14 a log to track, an analyst is going to go into the
15 database and do a search, make sure that those search
16 terms do not include PII and that they can provide us
17 with that log when we do our privacy compliance review.
18 So I think that provides us with greater
19 assurance. It provides the public with greater
20 assurance that they are focused on operationally
21 relevant activities.
22 So the next PCR, they will get a visit from me in

1 September 2012, and all of our public reports on
2 compliance reviews can be found on our Web site. And
3 I'd encourage you to take a look at all the NOC media
4 monitoring ones and the other ones that we have out
5 there on the Web.
6 If there are any questions, I'd be happy to answer
7 them.
8 MS. SOTTO: Thank you very much, Ms. Danker.
9 I'll kick off the questioning. With respect to
10 PCRs generally -- and Mr. Triner, this is no comment on
11 your program -- what tools do you have in place if
12 there is an egregious violation and you get only
13 limited cooperation from the program that you're
14 monitoring?
15 MS. DANKER: Well, I fortunately have not
16 encountered that because I think one of the things I
17 mentioned is you want buy-in. We have discussed that.
18 I think there would be instances where if we found
19 an egregious violation, that might kick into Mary
20 Ellen's investigative authority, and we'd kick that
21 over to conduct a formal investigation or refer it to
22 the Inspector General if that had to happen.

MS. SOTTO: Thank you.

Yes, Suzanne?

MS. BARBER: This is a previous request around -- making available some of the training. What does the PII certification training look like? Is it educating people about what is PII or --

MS. DANKER: Well, it educates on the seven permitted categories that they're allowed to collect PII, and then PII would be, you know, name, affiliation, publicly available user ID, and I can't remember the fourth data element. But just so the analysts know what they are allowed to collect on or, I'm sorry, what they're allowed to report on.

MS. CALLAHAN: It's pretty targeted, yes, for this type of training. Probably not useful for you guys.

MS. SOTTO: I'd like to ask another question. When you -- this is in reference to the retention of data. When you delete data that you shouldn't have taken in the first place, how do you ensure that you securely deleted that data from all sources, all repositories? Because I find that quite to be a challenging task.

MR. TRINER: Roger. Because the analysts have individual workstations that they share, so that workstation is fine. If they were working from the laptop, the laptop is brought in quarterly and then checked against anything that we had inadvertently. We know the size of our inadvertent releases are so small that it's easy to check individually by the date and time of that report and to make sure that they're out of there, as well as go back into our own data systems through our IT folks to make sure that anyone else who it was distributed to has that removed from that.

But again, part of the benefit of being so rigorous in what we're trying to do to make sure we're not going to really drive that, really question why we even have PII in there. So even though we had 20 percent had some sort of reporter name or -- I'm sorry. Not reporter. Mostly senior officials or spokesperson, even the last 2 months, that's trending down to less than 10 percent have those senior spokespersons or public affairs folks even mentioned in there.

MS. SOTTO: So you're following the dissemination

of data so that you can completely eliminate it. What about backup tapes?

MR. TRINER: That system is also purged at the same time. That's the easier part than that because we totally control those.

MS. SOTTO: Thank you.

Okay, we have a comment.

MS. CALLAHAN: I actually want to make one point about the four dates that are in the back of the privacy compliance review. Jamie and I had talked about having it be part of the compliance review and also to have it be part of the advocate meeting that we had.

And so, the randomly selected reports is true. It's random. But the four dates that are chosen are November 16th, my birthday.

(Laughter.)

MS. CALLAHAN: December 6th, the last DPIAC meeting. January 16th was the day that we launched the DHS portion of the DIB cybersecurity pilot, the JCSP, because I was looking to see if it was in there. The snapshot that we took actually didn't have it in there,

1 but it was, indeed, disclosed.
2 And then 1 day after -- February 21st, so 5 days
3 after I testified, 2 work days after I testified, just
4 to show the similarity, just to let you know. I'm sure
5 you didn't know what the dates were. But we were of
6 all dates, let's pick those dates as the example. So I
7 just want to let you know you guys were part of it.
8 MR. TRINER: Sorry I missed your birthday, Mary
9 Ellen.
10 (Laughter.)
11 MS. CALLAHAN: Seriously, Don.
12 MS. SOTTO: All right. Thank you very much. We
13 really appreciate it.
14 Oh, we have another question.
15 MS. GATES: I just had another quick question
16 about redress. You talked about you've got to depend
17 on the individual to go back to the source of the data
18 for redress, and that certainly makes sense. But in
19 your reports database, how are you maintaining
20 integrity there that let's say some inaccurate data
21 flowed into your reports, and then redress was taken
22 back at the source. How would you know that and deal

with that situation?

MR. TRINER: Okay. So, first of all, remember the PII we have in there is the spokesperson for the U.S. Government, large corporations. The vast majority of our reports are not individuals' names in there. So when we go through our process that when we would see that whatever was reported that someone brought to our attention that's not correct, we would then issue another report, and then that would be in the database as being correct.

It was still what was being reported in the media at that time. So that's the way -- it's sort of it's easier to issue an update than it is to try to go back and correct all that. Because we're really talking about was it maybe, perhaps was it Elm Street or was it Main Street? Was it a five-story house or a three-story house?

Because remember we're talking about the what, not really the who. So that's the process that we use.

MS. SOTTO: All right. Thank you very much, Mr. Triner and Ms. Danker.

As a quick housekeeping item, as a reminder, we

have a public comment period. If you haven't signed up and you would like to take part in our public comment period, please do so in the back of the room.

We will take a 9-minute break. We have eaten a bit into our break. So please be in your seats by 3:00 p.m. so we can proceed. Thank you.

(Break.)

MS. SOTTO: If the committee could please take their seats?

(Pause.)

MS. SOTTO: Would you please take your seats? We are delighted to welcome our Coast Guard representatives. We have Commander Pat Dibari, who is Deputy in the U.S. Coast Guard Office of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. Whew. Aptly shortened to C4ISR. Not so short.

We'd also like to welcome Marilyn Scott-Perez, Chief of the Office of Information Management. And Ms. Scott-Perez is the Coast Guard's Chief Privacy Officer, Chief Records Officer, and Chief FOIA Manager. Ms. Scott-Perez will talk to us about U.S. Coast Guard

maritime biometrics.

Commander Dibari serves as the Deputy of the Office of C4, Under Deputy Commandant for Operations in the Coast Guard. There are all kinds of other things that are just hard to say. So I will let you do it yourselves.

I just want to note one thing that I am so proud of. My firm has just signed on to be the only pro bono law firm for the Coast Guard. So we'll be doing a ton of pro bono work for the Coast Guard. So I'm delighted about that.

Welcome, and I'll turn the floor over to you.

MS. SCOTT-PEREZ: Can you hear me? Is it on? Is it working yet? Okay, good.

Thank you, Madam Chair, committee members, for hosting the Coast Guard today. We're looking forward to the discussion.

As she said, my name is Marilyn. I have brought my SMEs, my senior military experts with me. I have only been in the Coast Guard for about a year. In Coast Guard years, that's not a lot.

(Laughter.)

MS. SCOTT-PEREZ: So I do also want to take this opportunity to say from the Coast Guard and thank Mary Ellen for her leadership and her vision. It has been a thrill for me to have her mentorship for the last year. So we'll sorely miss her.

And with that, I'm going to turn it over to Commander Dibari.

COMMANDER DIBARI: Madam Chairman, ladies and gentlemen, it's a privilege to be here to brief you today. I'm going to talk about our Biometric Enabled Identity Program, and in doing so, I'd like to provide a little bit of context first with respect to the Coast Guard, recognizing that not everyone encounters Coast Guard every day.

So, in short, the Coast Guard has 41,000, roughly over 40,000 military members, 7,000 civilians, 8,000 Reservists, and approximately 30,000 auxiliary members that are volunteers for the Coast Guard to do search and rescue primarily and boating safety.

We have over 200 cutters, 1,800 boats, and over 200 aircraft. We operate in the U.S. inland waters, within our territorial seas out to 12 nautical miles.

We operate in the exclusive economic zone, out to 200 nautical miles on the high seas, as well as in the polar regions.

And historically, in 1790, we were part of the U.S. Revenue Cutter Service. What you hear as the modern-day Coast Guard was named in 1915, where it combined with the U.S. Lifesaving Service and 1939, the U.S. Lighthouse Service. And then, in 1940s, basically merged with the Bureau of Marine Inspection and Navigation, and today, we're under the Department of Homeland Security.

So we've had quite a history, and the reason why I'm bringing it up is because we do 11 missions, and the C4ISR part that we have a hard time talking about really helps us connect the dots and provide consistent, repeatable maritime safety and security throughout our 95,000-mile coastal border. So just to give a little context.

Today, I'm going to talk about the maritime domain, our authorities, the Biometrics at Sea program, and the privacy analysis, as well as our intentions to try to expand that within the operational context.

So the use of biometrics enhances our national security. It provides a tool to help detect known or suspected terrorists, national security threats while enabling law enforcement. Obviously, since the 9/11 Commission report was published, there is a national requirement to defeat terrorism at home and preempt threats to national security, help us connect the dots.

From the Coast Guard perspective, we need to identify and protect our Nation from dangerous people and improve maritime safety and security throughout our Nation while leveraging HSPD-24 and other authorities.

Just to give you some context on Coast Guard annual interactions, we do 64,000 vessel boardings a year. The Biometrics at Sea system is primarily focused on alien migration interdiction operations, where over 6,000 migrants are interdicted a year, trying to illegally enter the United States.

We also do over 73,000 TWIC verifications. There are 130,000 vessel arrivals greater than 300 gross ton, over 250 individual drug detainees, and over 6,000 fishing vessel boardings.

And as far as critical port entries and high-

1 interest vessel arrivals carrying certain dangerous
2 cargos, this gives a laydown of some of the arrivals
3 per year. As you can see from the diagram, our higher-
4 level arrivals are in the northern Gulf Coast, in the
5 port of Houston-Galveston, with 13,000 per year and 214
6 high-interest vessels per year. We also get a large
7 number in New Orleans, and you can see the other ports
8 listed.
9 Now with respect to authorities, the Coast Guard
10 has authorities with respect to port waterways and
11 coastal security, drug interdiction, aids to
12 navigation, search and rescue, living marine resources
13 to protect our fisheries within the exclusive economic
14 zone, marine safety, defense readiness, migrant
15 interdiction, marine environmental protection, ICE
16 operations, and other law enforcement.
17 We actually are officers of Customs. So we have
18 Customs authority under U.S. Code 19.
19 So the use of maritime biometrics, we first
20 conducted a pilot back in 2006, recognizing that we
21 were having a very big problem with illegal migration
22 of individuals from Dominican Republic into Puerto

Rico, and a lot of them were undocumented folks that were trying to get over in unseaworthy vessels. And we recognized that we need to evaluate the risk and intent of these unknown individuals in the maritime nexus and use that to help defeat -- enforce our laws and defeat criminal and terrorist activities.

In our process flow, we surveil, detect, classify biometric capabilities used to identify and prosecute. And specifically with our Biometrics at Sea pilot, you can see in the first portion of the process flow, Mona Pass, we typically have our 110-foot patrol boats patrolling. You can see the diagram there, the Mona Pass is between the Dominican Republic and Puerto Rico.

There was a lot of illegal migration. We patrol that area. We get aircraft support. They detect overloaded unseaworthy vessels, such as the picture you can see in Number 2. When they arrive, it's not like there's an immediate collection of biometrics.

Basically, the first thing we do is take care of the people that we encounter. They're typically unfed, exposed to the elements, and they need to be checked out. They're given a life jacket. So, typically,

they're not coming across on life jackets, and a lot of folks lose their lives trying to make this crossing not just from Dominican Republic, but also from other nations, such Haiti and Cuba.

So we are -- once we have the authority to collect, once we identified -- the boarding officers have identified that there's probable cause of illegal intent, we do a collection of biometrics. It's transferred onto a laptop. There's biographical data entry of the -- if there's -- if the person has, we know their name, gender, date of birth, their destination, intended destination. `That's basically loaded into the laptop and then transmitted via emails to US-VISIT, where it's searched and rolled into the database.

And then, at that point, there's a response given to the Coast Guard cutter as well as the Coast Guard command center in San Juan, and they're determined whether there's a hit against the database or not and the reference number. We basically put bracelets on the individuals with an ID number on it. And at that point, there's what's called a regional concurrence

1 team made up of the U.S. attorney's office, Border
2 Patrol, and Coast Guard to determine disposition.
3 At that point, we determine whether to repatriate
4 or prosecute individuals. Typically, if there's a
5 first violation, we will repatriate back to their
6 origin -- in this case, Dominican Republic -- and
7 provide them a notification that they have broken U.S.
8 law and identified that their biometric has been
9 enrolled into the US-VISIT database.
10 We advise of any redress process via the
11 DHS.gov/usvisit Web site, and then -- and basically
12 repatriate according to the operational commander's
13 direction. And prosecution is done based on U.S.
14 attorney's direction.
15 As far as operational policy, the Coast Guard
16 personnel involved in law enforcement operations may
17 only collect biometrics as part of the nationally
18 approved program or only approved on a case-by-case
19 basis by the Commandant. We do run into some
20 situations that would require it to be elevated, but
21 primarily, we collect biometrics if there's a crossing
22 or attempting crossing of the border or its equivalent,

if we reasonably suspect criminal conduct, or if there's consent voluntarily.

This gives you a little bit of context as far as the transit. From Dominican Republic to Puerto Rico, it's 71 nautical miles. And since the start of our pilot program, which has been operationalized, we've had over 4,000 biometric signatures collected and then over 1,000 matches, 861 prosecutions. And it's resulted in 80 percent reduction in illegal migration from Dominican Republic to Puerto Rico and roughly a 20 percent prosecution rate.

So we haven't collected very many biometrics, considering the number of encounters that we have annually. But the ones we have collected have been very effective in us being able to enforce U.S. law. It's also enabled us to determine who the smugglers are, who the bad actors are that are coordinating the operation.

And also it acts as a deterrent. So if we advise folks that this is not a safe thing, if you see, when you start the voyage, you may see it very calm outside. It could quickly whip up to high seas and overturn a

vessel and create a deadly situation.

To give context with our partner agencies, you can see CBP has approximately 80,000, 80,000 to 140,000 travelers per day. At 327 POEs, 1,000 per day are referred to secondary inspection due to biometric mismatch. USCIS, CBP, Border Patrol, ICE, and other agencies, you can see their numbers. Ours are a very small percentage compared to those. And as I've mentioned, 20 percent prosecution rate.

So it's a proven capability, and it's helping us to determine identity certitude in the execution of our mission.

With respect to privacy analysis, characterization of the information, it's minimally intrusive and collected while the person is onboard the Coast Guard cutter. We don't do it while they're on their dinghy. We take them onboard. We take care of them, and then we implement the system.

The use of the information is determined. If the persons interdicted at sea have been encountered within the IDENT database in the past, it's been very effective in determining repeat offenders. The data is

1 -- biometric information is retained only until the
2 appropriate information is confirmed and searched
3 against the database.
4 So once we know that US-VISIT has received the
5 electronic fingerprint transmission file, we swipe that
6 data clean off the device and off the laptops. It's
7 cleared off of there. So we don't retain any PII on
8 our devices or in our system. It's fully retained into
9 the US-VISIT IDENT system.
10 Sharing and disclosure. Privacy risks are
11 mitigated through data-sharing agreements via US-VISIT,
12 and audited access controls and reassuring limits and
13 controls are within that program. External sharing is
14 based on policies at US-VISIT and MOUs and the
15 information-sharing agreements we share with our
16 component agencies within DHS for the purposes of DHS
17 missions.
18 And notice minimum amount of information necessary
19 is collected, reviewed, and maintained. And access
20 redress, as I mentioned earlier, the redress procedures
21 are via US-VISIT, and only system of records to which
22 the U.S. Coast Guard will submit data for enrollment.

1 So with respect to technical access and security, IDENT
2 is the only system of record where we'll submit this
3 data for enrollment for the purposes of illegal
4 migration.
5 And all portable storage devices that contain
6 biometric data are encrypted, and access to the
7 equipment and data is strictly limited to need-to-know,
8 need-to-use basis.
9 Now we're also in the midst of a pilot project to
10 improve the capability. Right now, we're only able to
11 search the US-VISIT IDENT system. We're not able to
12 search FBI's IAFIS or DoD's ABIS system per HSPD-24.
13 So we only collect two index fingers and a photograph.
14 We would like to expand that to the 10 fingerprint,
15 which is the minimum standard for the IAFIS database.
16 And so, we're working on a pilot to do that.
17 We're examining iris collection in the cutter
18 environment. Naturally, as you can imagine, this is
19 not like a port of entry or an airport or seaport.
20 You're dealing with the direct sunlight. You're
21 dealing with the rolling and pitching in the sea.
22 You're dealing with sea spray.

1 But we still have done well as far as collecting
2 quality prints with slaps on the devices. And the
3 search would be extended via IDENT. The intent, the
4 desired end-state is via IDENT to IAFIS and ABIS
5 databases, and we're also evaluating usability of the
6 SEEKII device, which has been proven in the field by
7 other agencies as a good mobile biometric capability.
8 So, as I mentioned, the other databases,
9 effectively, we plan to leverage these existing
10 national technical capabilities -- effectively, 200
11 million records -- in order to perform our mission.
12 And you can see the type of information that's stored
13 on each database.
14 IDENT is primarily visa applicants traveling to
15 the United States, immigration violators, et cetera.
16 IAFIS stores folks that are arrested domestically,
17 limited to a number of individuals arrested
18 internationally, latent prints from crime scenes, and
19 ABIS are the bad actors and players overseas in Iraq
20 and Afghanistan, as well as latent prints from IEDs and
21 other hostile actions.
22 And of course, HSPD-24 calls for the Federal

agencies to "use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic contextual information of individuals." Right now, there are interoperability challenges between DoD ABIS and US-VISIT IDENT that are being worked through by the US-VISIT program.

Our goal is to basically mobily access that capability and provide feedback from these systems of record mobily to our operators in the field so that we can be effective in protecting our borders.

After we evaluated the pilot, we basically brought our interagency partners together and looked at what we've learned, capability gaps, and how we can improve that in the future, and this pictures provides a vision for where we want to go. It starts right in the middle, and really, as I mentioned, 95,000-mile maritime border is pretty difficult with only 244 cutters and over 200 aircraft.

So security is part of our vision, but it's balancing the need to move commerce, as well as protect privacy and protect our Nation. So guided by our laws,

1 policies, business rules, and doctrine, when we
2 encounter someone that we believe through probable
3 cause has violated, is intending to violate U.S. law
4 and make an illegal border entry, we do collect the
5 biometric. We also do local verification through the
6 TWIC program, which is indicated on there as well.
7 The biometric matching is done through the three
8 databases via satellite, and then we do an identity
9 intelligence analysis as well with our partners, and
10 the collaborative course of action or prosecution are
11 evaluated through the interagency collaboration. It's
12 called the regional coordination team.
13 And obviously, we're able to identify possible
14 known or suspected terrorists, national security
15 threats. We're able to nominate new KSTs, if
16 applicable. It provide us that tactical intelligence
17 to the operator, and we have encountered folks that
18 have false identities.
19 And also what we don't talk about often is the
20 need for force protection. So we'll encounter folks
21 that are previous felons, and we need to let our
22 operators know that are on scene right away that we do

have dangerous folks. So force protection is a big part of this as well.

And as far as our program planning, we're still collecting, looking to mature our CONOPS, and currently working our mission needs statement and acquisition documentation to move into a sustainable capability long term with integrated logistics support and so forth. And look to expand it beyond the current deployment.

Risk of inaction is missed opportunity to identify dangerous individuals along our maritime border, missed opportunities to identify and apprehend recidivist absconders and stowaways, and its potential of extending trust and access to the wrong persons or denying trust and access to the right persons. And it increases duration of operations, delays of commerce, as well as international trade.

A lack of threat awareness of Coast Guard forces, public safety, and national security, and noncompliance with the Coast Guard Authorization Act, which requires DHS to implement a maritime biometrics program in the maritime domain.

That concludes my presentation. I'd be happy to answer any of your questions.

MS. SOTTO: Thank you very much, Commander Dibari.

You may know that we -- half of this committee is taking a look at or thinking about privacy considerations and the use of biometrics for national security activities. So I think we'll have a lot of interest by this group.

Chris Pierson?

MR. PIERSON: Thanks.

First of all, thank you very much for your service. I appreciate that.

A quick question. In terms of the Coast Guard's mission is here, but also abroad. It does have deployments overseas. When it's working on those deployments in other hostile waters, is this biometric program being implemented alongside the military's program of biometric identification? Or is this more localized to the North American coasts?

COMMANDER DIBARI: We do have biometric capability deployed with our patrol force in Southwest Asia under NAVCENT control, and we do coordinate with the Navy as

1 far as CONOPS, concept of operations, and our
2 enterprise architecture very closely.
3 MR. PIERSON: And that's all as a part of -- I
4 mean, when the Coast Guard is deployed, it's deployed
5 under Homeland Security, but deployed in concert with
6 the military forces. But the Commandant's edict as
7 well as the authorization for the biometric still
8 extends out to those territorial waters as well?
9 COMMANDER DIBARI: Within the AORs that the Navy
10 and Coast Guard jointly operate in, that's correct.
11 MR. PIERSON: Thank you.
12 MS. SOTTO: I'd like to ask a question about
13 consent. You mentioned that consent is one of the
14 three ways that you collect prints. How does -- what's
15 the form of the consent? And do you inform the folks
16 who provide consent of the reason that you're talking
17 the prints and what you're going to be doing with the
18 prints?
19 COMMANDER DIBARI: I'm going to let our resident
20 lawyer answer that question. Lieutenant Aaron
21 Casavant.
22 (Laughter.)

LIEUTENANT CASAVANT: Yes, ma'am. Thank you.

The Coast Guard recognizes that informed consent is -- at times, it's a very factual dependent situation, and so we tend not to rely on individual consent. Although we recognize that if you were to fully explain the reason for collecting biometrics, why you were doing it and what you intended to do with the information that you could potentially get through informed consent, it's our intent not to use informed consent as a basis for collection.

Although we don't want to limit ourselves and say not address it, because I do think there's fairly clear authority that if you inform somebody about what you're doing and then ask for permission to do that particular technique and you get to a point where you have informed them about what you're doing, we don't want to limit ourselves. But we don't base our operations off of a consent basis.

MS. SOTTO: Thank you.

Greg?

MR. NOJEIM: Does the Coast Guard encounter U.S. citizens or people who claim they are U.S. citizens

trying to enter the country? And do you ever collect biometric information about those people whose claims of U.S. citizenship you question?

COMMANDER DIBARI: We handle that on a case-by-case basis. The intent of the program is not to collect on U.S. citizens for the purposes of illegal migration. The IDENT database is not set up to store, and I'm going to let Aaron answer that as well.

(Laughter.)

LIEUTENANT CASAVANT: Yes, sir. We do recognize that the IDENT database is a border control database. And as a result, again, if we have a suspicion of a person who is a U.S. citizen presents perhaps identification documents, passport, et cetera, or who claims to be a U.S. citizen, in other words, makes a claim but provides no documentation, at that point, that individual would be investigated likely without the use of biometrics to determine -- any database checks we do, for example, we'll take the individual's name and run them against other databases, not using biometrics, but using the biographic information that's provided.

Understanding that there may be additional risk. In other words, the individual could provide you with a false name or something along those lines. But again, the claim of U.S. citizenship, the program, as it's currently deployed, is intended to address our border control and border crossing authorities, sir.

MR. NOJEIM: Let me ask you a little more pointedly. If a person claims that they are a U.S. citizen, do they get a free pass so that their biometric identification is not collected?

LIEUTENANT CASAVANT: I think, sir, the concept of operations that we guide our forces by in the Mona Pass, in the South Florida AOR, if they were to encounter an individual on a boat of migrants, and there are, for example, 9 Haitians, 3 Dominican Republicans, and then 1 U.S. citizen, that individual's biometrics would not be collected, but we would still investigate that individual as a potential smuggler, migrant smuggler, taking advantage of his status in the U.S. to perhaps purchase a vessel, or otherwise, we've encountered situations where people steal vessels to do the migrant smuggling runs.

So that individual would still be investigated, but we would investigate that U.S. citizen the way we would investigate any suspicious U.S. citizen.

So, sir, to answer that question pointedly, no.

MS. SOTTO: Other questions? Suzanne?

MS. BARBER: Have you assessed the reliability of the biographical information that you gather that you associate with the biometric? The data you collect, my friends and I just say my name is Jane. Do I get away with that?

COMMANDER DIBARI: Yes, I think in some cases we determine through the identity analysis and intelligence analysis that the person basically falsely gave their information or has multiple false identifications. So, yes, we do assess that through the other pieces, which is the identity intelligence check against law enforcement and foreign intelligence open source databases.

MS. BARBER: The security around the email transmission. So just -- you just say you email the prints back?

COMMANDER DIBARI: It's basically within the Coast

Guard network, which is a secure network.

MR. NOJEIM: One more question. Give us the numbers that in an ideal world you would want to be able to biometrically identify. Are you looking at tens of thousands, or are you looking at just thousands?

Right now, you identify how many in a year biometrically? You, meaning Coast Guard.

COMMANDER DIBARI: So the numbers show roughly 4,000. We've done this for 6 years. So under 1,000 a year. But it's not like we have a projection that we shoot for. We go out and do our operation, and we determine if -- first of all, the boarding officers do an initial safety inspection and try to determine who we're encountering and where they're coming from, where they're going.

And build, if we suspect illegal activity, we try to build probable cause if there's illegal activity happening and then use the capability to certify identity if our -- consistent with our business rules.

MR. NOJEIM: Is the 4,000 roughly the scope that you need, and you don't really need to scope up a lot

1 higher than that?
2 COMMANDER DIBARI: Well, we don't know what we
3 don't know. I think right now in the past, we've used
4 the biographical method that Lieutenant Casavant
5 mentioned, and multimodal biometrics enables more
6 identity certitude.
7 So do we need to scope up further? There could be
8 other threat factors where folks have -- are trying to
9 illegally enter the United States or conduct other
10 illicit activities, such as on the northern border or
11 southwest border.
12 MS. GATES: You talked about redress being through
13 typical the US-VISIT procedures and on the Web site.
14 But on a practical level, these individuals that are
15 picked up on these kinds of boats, how do you provide
16 that sort of notice and help them to understand what
17 their rights might be?
18 COMMANDER DIBARI: Practically speaking, we
19 basically provide them a piece of paper that's got that
20 notice on it. And on the opposite side, it's in
21 Spanish. So it's English and Spanish.
22 MS. SOTTO: Linda, then Marjorie.

MS. KOONTZ: Can you tell me how often individuals have sought redress under this program, and what the results of those actions were?

MS. SCOTT-PEREZ: If I can turn my microphone on, can you hear me?

We wouldn't have insight into that because it has to go directly to US-VISIT for the redress. So the Coast Guard would not know that.

MS. CALLAHAN: So US-VISIT has redress opportunities where people would amend the records. It could go two different ways. One through FOIA by looking at their record and asking about it and then realizing that there's a problem, and one by saying I'm having a problem at the border.

Mr. Dibari pointed out that Coast Guard or, sorry, CBP may have referrals to secondary because of mismatches. US-VISIT has about hundreds of times where they had mismatches where people have sought redress each year, approximately. But it's in that spectrum.

MS. KOONTZ: Thank you.

MS. CALLAHAN: And they're obviously not all related to the Coast Guard, which is just a small

1 percentage of that.
2 MS. WEINBERGER: Okay. Here we go. Not that I
3 need it because, honestly, I can be heard.
4 I thank you for your patience and your answers to
5 questions. I'm sure this is not the best part of your
6 day.
7 I do have a quick question to you. I noticed the
8 biometrics you are obtaining include not just
9 fingerprints, but photographs as well. I'm assuming
10 you're using that for some kind of facial recognition
11 input. Is that correct?
12 COMMANDER DIBARI: No. It's just for context.
13 MS. WEINBERGER: So it's not being used for any
14 other cross-referencing databases?
15 COMMANDER DIBARI: It could be accessible from
16 other inquiries into the tied-in database, based on the
17 information-sharing agreement.
18 MS. WEINBERGER: Used, say, with other entities.
19 They would be able to access, say, that photograph and
20 run it through visual recognition for their own
21 legitimate purpose under the MOU?
22 MS. CALLAHAN: Hello.

(Laughter.)

COMMANDER DIBARI: No.

MS. CALLAHAN: This is a US-VISIT question. US-VISIT's database does not -- can you hear me, transcriber? Transcriber, you're okay? Good.

US-VISIT's database does not utilize visual recognition tools. And so, neither the Coast Guard when they receive it or US-VISIT when they're looking at it, the only biometric that they're comparing in an automated fashion is the fingerprints, whether it's 2 print or 10.

They do do an ID check. Like if Mr. Dibari's fingerprints were associated with Ms. Scott-Perez, then you go and say, well, that actually doesn't look like that matches. And that's some of the redress that we have is husbands and wives will get switched up, people who are in line one after the other may get switched up, and that's the type of redress.

But it's only for kind of optic reasons to go and look does this person physically resemble? There is not facial recognition utilized within IDENT. So no MOU would have authorized that on their own.

MS. WEINBERGER: Okay.

MS. SOTTO: Howard Beales?

MR. BEALES: I'm interested in the scope question. It sounds like you're only using this in the border crossing context. Is -- I mean, suppose you encounter a boat that's got potential illegal immigrants. It's also got U.S. citizens. It's also got drugs.

Do the U.S. citizens, under what circumstances do you fingerprint the U.S. citizens in that kind of encounter?

LIEUTENANT CASAVANT: Yes, sir. Thanks for the question. It is a good question because we recently had an issue where there was a vessel in the Mona Pass that was initially suspected.

A migrants' moment, but instead turned out that it was smuggling drugs. And what were originally thought to be migrants' personal effects were, in fact, 300 kilograms of cocaine, necessitating a switch from a migrant response framework to a counterdrug response framework.

So the question is an excellent question. We are not restricted to one way to break the U.S. law.

(Laughter.)

LIEUTENANT CASAVANT: So, in that context, it's likely that if we do discover drugs, the Maritime Drug Law Enforcement Act framework would be initiated. And so, if you did have U.S. citizens, which those individuals are subject to the Maritime Drug Law Enforcement Act, at that point, those individuals would be subject to processing just the way we would handle suspected, other suspected U.S. citizens.

So that would be, in effect, separated because those individuals would be subject to prosecution in the U.S. anyway. In other words, the collection of biometrics is not assisting the Coast Guard because the law enforcement operations are already proceeding. Your vessel is subject. You are subject to the Maritime Drug Law Enforcement Act.

There is no benefit to be derived through collecting biometrics at sea because it's not helping us arrive at a disposition decision. This is unlike the biometrics at sea in the Mona Pass, where we collect biometrics at sea and it helps our partners, the U.S. attorney's office, decide whether or not we

want to prosecute this individual for repeat violations of the U.S. immigration law.

So I would say that in separating the two -- we would separate the two, and we would say, okay, we've got folks that are suspected of violating migrant smuggling laws and perhaps drug smuggling laws at the same time, engage with the interagency partners to see, okay, is everybody suspected of drug smuggling, or we're doing two separate type of investigations?

And that would also be largely determined by the boarding officer and boarding team, what their on-scene investigation reveals as well. So does that help, sir?

MR. BEALES: Okay. Just to make sure I understand. So, basically, what would happen is you find drugs. You investigate the U.S. citizens as you would any other U.S. citizen. At some point, there may be a decision to arrest or prosecute, or is it do you not have arrest authority? Or is it analogous to arrest?

LIEUTENANT CASAVANT: Sir, what we do is we detain at sea in lieu of arrest. And so, how that works is it's largely driven by the flag state of the vessel.

1 Our jurisdiction is tied to the flag of the vessel.
2 Under international law, vessels exercising
3 freedom of navigation on the high seas are subject only
4 to the jurisdiction of the flag state. And so, when we
5 take law enforcement action against a particular
6 vessel, one of the key things that we focus in on is
7 what is the flag state of that vessel?
8 So if it's a U.S. vessel registered in the United
9 States or one of the 50 States, if it's a U.S. vessel,
10 the Coast Guard has jurisdiction over that vessel
11 anywhere on the high seas. You heard Commander Dibari
12 mention some of the jurisdictional zones -- territorial
13 seas, contiguous zone, exclusive economic zone, and
14 then high seas.
15 So regardless of where that vessel is located, we
16 have jurisdiction over that vessel, and the Maritime
17 Drug Law Enforcement Act subjects the entire vessel to
18 the operation of the MDLEA such that when we tell our
19 DOJ partners about this particular case that we have
20 ongoing, they will likely be interested in prosecuting
21 this case under the MDLEA.
22 MR. BEALES: Okay. And then when it gets to that

point, presumably, that person is fingerprinted and checked against --

LIEUTENANT CASAVANT: And again, the Coast Guard wouldn't be doing that.

MR. BEALES: I see.

LIEUTENANT CASAVANT: Because there is a desire to bring them back for prosecution. And again, there would be no purpose for the Coast Guard to do that at that point because we're not driving any kind of disposition determination at sea.

MR. BEALES: Okay. When you say there were 1,000 or so matches out of these 4,000 or so biometrics collected, that means basically a hit against a US-VISIT database?

COMMANDER DIBARI: Yes, sir.

MR. BEALES: Okay. Thanks.

MS. SOTTO: Joanne?

MS. MCNABB: Were the other 3,000 then put into the database?

MS. CALLAHAN: So, Joanne, I think it's 1,000 of the 4,000 collected are repeat collections. Right, Commander Dibari? So you have a recidivist percentage

of 25 percent.

COMMANDER DIBARI: That's correct.

MS. CALLAHAN: But all 4,000 go into IDENT.

MS. MCNABB: All of them go.

MS. SOTTO: Suzanne, did you have another question?

Any additional questions?

(No response.)

MS. SOTTO: All right. We're very grateful for your time. Thank you very much for joining us.

COMMANDER DIBARI: You're welcome. Thank you.

MS. CALLAHAN: Madam Chair, for the record, 1,356 requests for redress to US-VISIT last year overall. So in the hundreds, but 1,300 is -- 1,356, and it will be in Jonathan's annual report, which will come out in September.

MS. SOTTO: All right. We are now at the public comment portion of our day. If there are any members of the public who would like to address the committee, I would ask that you come forward at this point.

Do we have anybody who is signed up? No.

(No response.)

MS. SOTTO: Okay. And if there's nobody who wants to come forward with public comments, then I will thank all of our speakers for the day. We very much appreciate your attending and helping us understand the programs that are so important to you.

This concludes the public portion of today's meeting. We are grateful for all of your interest in our work and the work of the Privacy Office.

The minutes of the meeting will be posted on the Privacy Office's Web site at www.dhs.gov/privacy in the near future, and we certainly encourage you to follow the committee's work and to check back frequently. We do good things, and we are prodigious in our writing.

I would ask members of the public to now take their leave. The committee is going to begin a brief administrative session. So please, committee, sit tight.

Once again, I extend our committee's thanks to the speakers and want to applaud Mary Ellen's great work.

(Applause.)

(Whereupon, at 3:51 p.m., the meeting was concluded.)