

1 MEETING OF THE
2 DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

3
4
5 Tuesday, September 28, 2010

6 United States Government Printing Office

7 Carl Hayden Room

8 732 North Capitol Street, N.W.

9 Washington, D.C. 20401

10
11
12 The meeting was convened at 8:41 a.m.,

13 RICHARD PURCELL, Chair, presiding.

1 DPIAC COMMITTEE MEMBERS PRESENT:

2

3 RICHARD V. PURCELL, Chair, presiding

4 ANA I. ANTON

5 RAMON BARQUIN

6 DANIEL W. CAPRIO, JR.

7 RENARD FRANCOIS

8 JAMES W. HARPER

9 KIRK HERATH

10 DAVID A. HOFFMAN

11 LANCE HOFFMAN

12 JOANNE MCNABB

13 CHARLES PALMER

14 NEVILLE PATTINSON

15 JOHN SABO

16 LISA J. SOTTO

17

18

19

20

21

22

1 P R O C E E D I N G S

2 MS. LANDESBURG: Good morning everyone, I am
3 Martha Landesberg, Designated Federal Official for the DHS
4 Privacy and Data Integrity Advisory Committee.
5 Welcome, everyone, to the third quarterly meeting of
6 2010. I'll now turn over the meeting to our
7 Chairman, Richard Purcell.

8 MR. PURCELL: Thank you, Martha. And
9 welcome, Committee members. It's delightful to see
10 you all here again. We open our meeting today as
11 usual, with some housekeeping tips, which include,
12 please, silence your mobile devices in such a way as
13 to not interrupt our erudite discussions.

14 We also have reserved time at the end of the
15 -- at the midday period, 11:30 to noon. If members of
16 the public are interested in addressing the Committee
17 at that time, please sign up. There's a table outside
18 this room for that purpose.

19 As is our custom, we welcome Mary Ellen
20 Callahan, the DHS Chief Privacy Officer, to our
21 meeting first thing, for an update from the Chief
22 Privacy Officer. Ms. Callahan has served as the Chief

1 Privacy Officer of the Department since March of 2009.

2 Amazing, huh?

3 MS. CALLAHAN: How time flies when you're
4 having fun.

5 MR. PURCELL: Time flies. Prior to joining
6 DHS Ms. Callahan specialized in privacy, data
7 security, and consumer protection law as a partner at
8 Hogan & Hartson in Washington, D.C., and also has
9 served as the co-chair of the Online Privacy Alliance,
10 and as vice-chair of the American Bar Association's
11 Anti-Trust Division Privacy and Information Security
12 Committee.

13 We all know Mary Ellen and her Privacy
14 Office team, and we know that they are responsible for
15 privacy compliance across the entire Department. I
16 want to also make sure we remind ourselves that Ms.
17 Callahan also serves as the Department's Chief Freedom
18 of Information Act Officer.

19 Ms. Callahan, we are delighted to see you
20 this morning. Thank you, please proceed.

21 MS. CALLAHAN: Thank you, Chairman Purcell.
22 Good morning, everyone. Good to see everyone.

1 First, I wanted to give a brief overview of
2 today's meeting. I'm going to begin with an overview
3 of the Privacy Office activities since our last
4 meeting on May 25th, as Richard mentioned. As usual,
5 there's a lot going on in this area, and I'm pleased
6 and proud to give you a picture of how hard and
7 effectively my staff has been working.

8 Then Jamie Pressman, who is an Associate
9 Director of our Compliance Group, will brief you on
10 our efforts to bolster accountability for privacy
11 throughout the Department by conducting compliance
12 reviews. As you know, this is one of my major
13 initiatives, and I'm very pleased with Jamie's
14 leadership in this area.

15 After the break, Steve Richards, our
16 Associate Director for Communications and Training,
17 will provide an overview of privacy training in the
18 Department in response to the Committee's request.
19 Our training programs are always evolving, and Steve
20 will update you on the direction they are taking.
21 Steve is showing great leadership in trying to
22 leverage best practices across the Department to

1 systematize it and to find innovative ways to do adult
2 training. So we're very excited about that.

3 And our last speaker will be Larry Castelli,
4 Privacy Officer for Customs and Border Protection, who
5 will speak on CBP's implementation of DHS Privacy
6 Policy. He is the second or third, depending on how
7 you're counting, of our ongoing series of DPIAC
8 briefings by DHS component privacy officers. I'd like
9 to thank Larry, Jamie and Steve for their efforts to
10 provide the Committee insight into their work.

11 Before I start the official kind of
12 presentation, I wanted to remind the Committee that
13 one of the goals of the Secretary and the Deputy
14 Secretary is to make sure there are senior federal
15 officials that lead the privacy policy of each of the
16 components of the Department.

17 And as of today, we've added two new privacy
18 officers since the DPIAC meeting in May. Over my left
19 shoulder is Emily Andrew, who is the privacy officer
20 for NPPD, the first privacy officer that they have had.
21 NPPD, as you know, oversees a wide variety of issues
22 that will have impact on privacy and personal

1 security, one being cybersecurity. So NPPD is with
2 CS&C as well as the Federal Protective Services, FPS,
3 that guard federal buildings, and a whole host of
4 infrastructure issues and other elements.

5 As many of you are aware, Emily is a legend
6 in the federal privacy community, having served as the
7 Chief Privacy Officer for both the U.S. Postal Service
8 as well as the Department of State. So we are
9 thrilled that Emily has joined the DHS family. In
10 addition, the Office of Intelligence and Analysis,
11 I&A, has a new privacy officer who I don't think is
12 here yet, but she is expected to attend as well.

13 Claire Barrett previously had served as the
14 Deputy Chief Privacy Officer for the Transportation
15 Security Administration and again, has a long history
16 in privacy and federal privacy practice, as well as
17 her graduate work on the intersection of privacy and
18 intelligence. So she is, I think, absolutely
19 perfectly suited to take on this important task in the
20 Office of Intelligence and Analysis.

21 And by the time I speak to you in December,
22 we will have completed all the privacy officers, as

1 the Directorate of Science and Technology I believe
2 has made a selection on their privacy officer. So we
3 will be complete, and we're thrilled with the new
4 additions as well as with the ongoing support that the
5 component privacy officers give us every day in
6 integrating privacy throughout the programs of DHS
7 from the very inception. So I wanted to welcome them
8 to the family.

9 And now if I could start the official
10 portion of my presentation.

11 MR. PURCELL: Please.

12 STATEMENT OF MARY ELLEN CALLAHAN, CHIEF PRIVACY
13 OFFICER, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

14 MS. CALLAHAN: The first thing I wanted to
15 talk about today is what Richard mentioned, which is
16 the Freedom of Information Act. As you know, I do
17 serve as the Chief Freedom of Information Act Officer.

18 The Freedom of Information Act is -- the
19 number of our access requests are judged on a fiscal year, which
20 is going to end on Thursday. So we are really in the
21 sprinting element of the Freedom of Information Act
22 work.

1 The Disclosure and FOIA Group has worked
2 laboriously this year to make sure that the FIPPs
3 Transparency principles are integrated and to make
4 sure that indeed we are addressing the Open Government
5 Directive's elements that are associated with the Freedom
6 of Information Act.

7 DHS has always received an incredible number
8 of Freedom of Information Act requests. Last year for
9 the fiscal year we received 103,000 Freedom of
10 Information Act requests. By the end of August of
11 2010 for the fiscal year we had received over 120,000
12 FOIA requests.

13 We'll probably see an increase of between 25
14 and 33 percent of Freedom of Information Act requests
15 for this fiscal year, which is an extraordinary
16 increase for a department that receives numbers of
17 this size.

18 The Freedom of Information Act process,
19 we've been trying to, not centralize but systematize
20 the process because each of the components, like
21 privacy officers, have FOIA officers working on their
22 specific elements and their specific types of

1 documents.

2 With that said, I want to thank all the FOIA
3 officers. They have done Herculean tasks, because
4 that 25 percent increase has gone pretty much across
5 the board in the Department.

6 The biggest number of increases is in USCIS,
7 who receive the most types of requests usually Privacy
8 Act requests, for people seeking their immigration
9 files. In August, CIS received over 10,000 Freedom of
10 Information Act requests themselves, which is the
11 first time that they have hit five digits.

12 With that said, we are likely going to meet
13 our stated goal of reducing the backlog 15 percent
14 this year. So we're seeing a 25 to 30 percent
15 increase, and yet we should be able to reduce the
16 backlog by 15 percent, thanks to extraordinary
17 efforts, as I said, by the FOIA officers and FOIA
18 professionals throughout the Department.

19 And I want to thank them for that and their
20 hard work. They are not going to be here today
21 because literally every second counts in terms of
22 closing out the responses and making sure that we are

1 being good stewards of the public in responding to
2 requests for information.

3 In addition, other elements on the Freedom
4 of Information Act, the Disclosure and FOIA Group, we
5 completed two major compliance-related milestones this
6 past year, one being our draft FOIA Privacy Act System
7 of Records Notice, which was published in October of
8 2009, and became final in August. The SORN updates an
9 existing legacy SORN.

10 And then in August I signed a related DHS-
11 wide Privacy Impact Assessment covering all systems
12 used to collect data for the purpose of processing
13 FOIA requests. The PIA applies a programmatic
14 approach analyzing the privacy risks associated with
15 our FOIA and Privacy Act Program and the steps we may
16 take to mitigate those risks.

17 So that's yet again, another example of
18 trying to systematize and leverage best practices
19 across the Department as we work on these issues
20 together.

21 With regard to the privacy portion of my
22 office, we've had a great deal of action on that side

1 as well. The Office released our 2010 annual
2 report to Congress on September 17. You'll find a
3 copy in your folder, and there are copies outside for
4 the public. The report is a comprehensive review of
5 our activities between July 1, 2009 and June 30, 2010.

6 And it discusses many of the themes that
7 I've talked to you about, including the ways in which
8 our office has demonstrated leadership by systemizing
9 privacy protections throughout the Department, by
10 participating in interagency efforts to embed privacy
11 protections throughout the federal government, and by
12 advancing international privacy through intensive
13 outreach and dialog with the Department's partner
14 countries and allies.

15 I'm also very pleased to announce that as of
16 yesterday, Debbie Diener, formerly the Director of the
17 IRS's Office of Privacy Policy, has joined us as
18 Senior Advisor and Director of Privacy Policy. She's
19 in DHS new hire training today, so you won't have an
20 opportunity to meet her for those of you who don't
21 know her.

22 But she is again a great asset to the

1 Department. She's an accomplished privacy lawyer, and
2 we look forward to working with her on a great deal of
3 items. She also is again well-known in the privacy
4 community, so I think she's an outstanding, not
5 replacement -- you can't replace Toby -- but she's an
6 outstanding complement to my office overall, and we
7 look forward to working with her.

8 With regard -- something else that we have
9 done, which I think I'll talk about a little bit later
10 as well, which is we have produced in June a guide to
11 the DHS Privacy Office, which is kind of an FYI in
12 terms of what my office does, how does it address
13 elements, what does it work with, and how does it
14 prioritize the issues that are before it.

15 And that guide has been a very useful tool,
16 both for us in trying to explain what the Office does,
17 because sometimes that's not clear, particularly maybe
18 to our European colleagues, but also secondarily to
19 help provide a guide to others who are trying to
20 establish privacy programs, whether it be at the
21 component level or at the Department level for some
22 agencies who are considering adding privacy officers.

1 And I think it can be a good tool just in
2 terms of establishing a privacy program at large,
3 whether it be in a private sector or in a public
4 sector office. So we did great work on that. I want
5 to thank Martha for her leadership on that project as
6 well.

7 With regard to privacy compliance, they of
8 course have been hard at work reviewing DHS systems
9 and programs through the Privacy Threshold Analysis
10 and overseeing the drafting of Privacy Impact
11 Assessments and SORNS.

12 Since the Committee last met, we have
13 approved 202 PTAs and published 20 Privacy Impact
14 Assessments, three System of Records Notices, two
15 Notices of Proposed Rule Making to Implement Privacy
16 Act Exemptions, four Rules to Implement Privacy
17 Exemptions, and a partridge in a pear tree.

18 [Laughter.]

19 MS. CALLAHAN: You were thinking it, weren't
20 you?

21 MR. PURCELL: I was.

22 MS. CALLAHAN: You were, I knew it.

1 Just a couple of highlights on the
2 compliance side. The published Privacy Compliance
3 documentation includes a PIA and System of Records
4 Notice for USCIS's Citizenship and Immigration data
5 repository, also known as CIDR, which is hosted on
6 DHS's classified networks and makes information from
7 the USCIS Benefits Administration systems available
8 for query by authorized USCIS personnel.

9 And a SORN for DHS's forthcoming
10 participation in the National Suspicious Activity
11 Reporting Initiative or NSI. We will have a related
12 Privacy Impact Assessment release next month, and I'll
13 probably talk about the SAR initiative in the December
14 meeting. But I'm happy to field questions on that, if
15 you have any at this time.

16 We've also reviewed 91 major IT investments
17 through the budget process and failed 11 of those
18 systems for lack of privacy compliance documentation.

19 Programs that fail receive higher scrutiny by
20 component and DHS leadership, and of course are not
21 able to be implemented until those modifications have
22 been made. We're actively working with the relevant

1 component privacy officers and program managers to
2 make sure that those modifications and documentations
3 are indeed addressed.

4 DHS will be reporting its FISMA score to OMB
5 at the end of the month. DHS has spent the last year
6 updating its IT inventory and bringing all components
7 into compliance. Overall, DHS's FISMA PIA score
8 improved from 67 to 70 percent and its FISMA SORN
9 score from 93 to 94 percent.

10 We will continue to work with the components
11 that need to improve their scores, and trust me, I'll
12 be focusing on the ones that are delinquent very
13 thoroughly for the next fiscal year, and you'll be
14 able to see who those are at the end of the month.

15 Finally, as you'll learn later this morning
16 from Jamie, we've recently published our first Privacy
17 Compliance Review, which was a review of the
18 Department's use of social media for situational
19 awareness during the Winter Olympics and after the
20 Haiti earthquake. So you'll hear about those, that
21 executed review as well as our plans for the future.

22 For our Privacy Technology Group, we've been

1 actively engaged in several fronts since the Committee
2 last met. In the area of cybersecurity the group
3 continues to participate in coordinating committees
4 involving the various cybersecurity program offices,
5 both within and outside the Department, including
6 close coordination with the National Protection and
7 Programs Director at the Office of Cybersecurity and
8 Communications, which I mentioned earlier, the
9 Information Oversight Officer at CS&C, to identify
10 alignments between that office's work and my office's
11 privacy compliance activity.

12 And the way I see it is kind of a multi-
13 layered approach, with us taking periodic reviews and
14 Emily, the CS&C Information Oversight officer, and so
15 on, taking more of the day-to-day review, and we'll
16 make sure that the compliance and the oversight is
17 appropriately formulated. And we look forward to
18 working with Emily on these issues going forward.

19 The privacy technology team has also been
20 working on developing an enterprise approach to our
21 privacy compliance work with the Science and
22 Technology Directorate. At this moment we're focusing

1 on the Department's use of volunteers and research
2 projects in terms of having a systemwide Privacy
3 Impact Assessment with standards enumerated therein so
4 you don't have to do a Privacy Impact Assessment each
5 time you have volunteers, if indeed they comply with
6 the stated standards in the Privacy Impact Assessment,
7 trying to systematize the application while also
8 avoiding the paperwork process if it's just for
9 paperwork.

10 And then in support of the President's Open
11 Government Initiative, we also continue to review with
12 the DHS Office of the Chief Information Officer, to
13 review all DHS data sets proposed for posting on the
14 Data.gov web site, and with the Office of the Chief
15 Financial Officer to review data sets proposed for
16 publication on the USAspending.gov. We have to date,
17 reviewed 51 data sets proposed for Data.gov and 15
18 data sets for USAspending.

19 With regard to Privacy Incidents and
20 Inquiries, we've had quite a busy time with that as
21 well. The Privacy Incidents and Inquiry group held
22 its third privacy incident handling quarterly meeting

1 on June 29 to discuss privacy incidents at DHS that
2 took place between February and March 2010.

3 In addition, on September 14th I hosted the
4 second annual privacy incident management meeting of
5 the DHS Core Management Group, which includes DHS
6 senior leadership, component privacy personnel,
7 component information technology, security personnel,
8 and was led by myself as Chief Privacy Officer and by
9 Richard Spires as Chief Information Officer.

10 At the meeting itself the Incidents and
11 Inquiry Group provided a detailed comparison of FY2009
12 and FY 2010 incidents, and conducted a root cause
13 analysis to determine where the incidents were
14 occurring, to target areas of vulnerability and to
15 direct training as appropriate, in order to lessen the
16 likelihood that incidents will occur.

17 In addition to these events and the ongoing
18 work that the Incidents and Inquiry Group does, we
19 also are conducting a broader scale investigation of a
20 data breach that has some policy implications, and
21 that should be released by the time that you are -- by
22 our December meeting.

1 You're going to hear from Steve later on in
2 terms of Privacy Office communications, but we continue
3 to work to expand our public outreach efforts. We
4 have developed an external communication plan that
5 Steve has led, to raise public awareness of our work,
6 both in the privacy community and in the general
7 public.

8 The plan includes leveraging our web site to
9 make sure that the public is aware of our PIAs, SORNs,
10 public events, reports and other publications,
11 periodic e-mail campaigns to our constituents that
12 just kicked off this month, where we had two e-mail
13 campaigns, one introducing the concept of the e-mail
14 blasts and introducing the guide itself, and of course
15 offering an opportunity to opt out.

16 And then we last week, sent out a notification
17 about the Annual Report. I don't anticipate we'll do
18 such frequent e-mails. It just happened that we were
19 launching this and the report was coming out the same
20 time. We're also looking at occasional articles in
21 the DHS Blog, presenting my thoughts on privacy issues
22 that may be of public interest.

1 Other areas where we're working on an
2 interagency basis include the Chief Information
3 Officer Council, the Privacy Committee therein. We
4 continue to be very engaged in that work on many
5 levels. As you may recall, I serve as the co-chair of
6 the Council's Privacy Committee and several members of
7 my staff are members of the subcommittee as well.

8 My Deputy, John Kropf, co-chairs the
9 International Privacy Subcommittee with the Department
10 of State, and that subcommittee has undertaken several
11 new projects, including collaboration on an article
12 for European audiences on how the U.S. uses compliance
13 documentation to increase accountability, and
14 development of an international privacy law matrix
15 that will be used in international negotiations where
16 information sharing and privacy concerns are raised.

17 And our own Martha Landesberg, our Associate
18 Director for Policy, also in addition to running DPIAC
19 and doing the Annual Report and working on the Data
20 Mining Report, in her spare time, she co-chairs the
21 Best Practices Subcommittee with the FDIC and the
22 Department of Energy.

1 The subcommittee led the drafting of the
2 Privacy Committee's *Elements of a Federal Privacy*
3 *Practice*, a comprehensive guide to building an
4 effective agency program, which was issued in June.
5 You'll find a copy in your folders, and they are
6 available for the public outside.

7 The subcommittee has developed a very
8 ambitious project plan for FY11 and '12, we got
9 to discuss it just yesterday, that includes guidance
10 on recognizing privacy risks when carrying out Privacy
11 Impact Assessments, on conducting an inventory of
12 Agency holdings on Privacy -- PII, and on drafting
13 effective agency notices.

14 The Elements document, in coordination with
15 the DHS Guide to the DHS Privacy Office, help provide
16 a framework for federal privacy offices and are indeed
17 seem to be -- they were created to be symbiotic in
18 terms of both the big picture elements while the guide
19 talks about the nuts and bolts of how DHS does their
20 specific implementation of privacy protections.

21 As directed by the Deputy Secretary, we
22 continue our review of intelligence products prepared

1 by the Intelligence and Analysis component for
2 privacy -- we continue to do the review for privacy
3 issues. Since May we've reviewed approximately 80 INA
4 analytical products and 200 Homeland Intelligence
5 Reports.

6 This is another way that my office works to
7 further privacy protections and make sure they are
8 embedded throughout the Department. At this moment
9 I'd like to take a -- I actually am not going to say
10 something. I've decided I'm not going to say
11 something, because there's something that is not yet
12 public, but I will make the statement in December.
13 But we continue to work on the reviews of I&A
14 products.

15 Relatedly, we also work and also are deeply
16 engaged with the work on Fusion Centers. As you know,
17 I have a statutory responsibility to make sure that we
18 have met our training responsibilities, and I'd like
19 to go through the three different ways in which we
20 are meeting those goals.

21 There are 72 designated Fusion Centers
22 across the United States. Sixty-three of these have

1 I&A representatives assigned to them. Under the 9/11
2 Commission Act, the Privacy Office, together of course
3 with our counterparts in the Office of Civil Rights
4 and Civil Liberties, is responsible for providing
5 these intelligence professionals with privacy and
6 civil rights/civil liberties trainings before they
7 depart.

8 We continue to provide the privacy training
9 as new analysts join the Office of Intelligence and
10 Analysis. And as I discussed with the Committee in
11 May, we are also providing training to state and local
12 Fusion Center representatives.

13 We approach this training in a couple of
14 different ways. First, we train Fusion Center Privacy
15 Officers in techniques they can use to provide privacy
16 training in their own centers. This effort was well
17 under way when the Committee last met.

18 In four sessions at regional Fusion Center
19 conferences across the nation and one makeup session
20 here in Washington, we have trained privacy and civil
21 liberties officers at 69 of the 72 Fusion Centers, so
22 that they can then go and implement privacy and civil

1 liberties training at their own Fusion Centers going
2 forward.

3 Our engagement with these newly appointed
4 privacy officers will, of course, continue, and we're
5 busy supporting their efforts to build robust local
6 privacy protection programs. My office, together with
7 the Office for Civil Rights and Civil Liberties, also
8 provides in-person training, where we travel to Fusion
9 Centers and provide a comprehensive introduction to
10 federal perspectives on protecting privacy, civil
11 liberties and civil rights in the Information Sharing
12 Environment.

13 The training is meant to support the in-
14 house training program now being developed by each
15 Fusion Center privacy and civil liberties officer,
16 but they are meant to be complementary. The trips,
17 the kind of in-person training, were temporarily on
18 hold while we focused on this heavy lift of training
19 the trainers sessions. But as soon as we were done with
20 the training the trainers sessions we were back on the
21 road.

22 Since our last meeting CRCL and the Privacy

1 Offices have conducted in-person training to seven
2 centers in two states. Trips are planned through
3 November to New Jersey, Delaware, North and South
4 Carolina, Ohio and Oklahoma.

5 If you notice, no warm states there. I'm
6 not letting them do any boondoggles. We're making
7 sure that we're being effective in trying to address
8 the Fusion Center needs as we reach out to these
9 Fusion Centers.

10 On a related note, as the Committee is very
11 aware, we continue to review Fusion Center privacy
12 policies to confirm that they are at least as
13 comprehensive as the federal privacy guidelines for
14 the information sharing environment.

15 As you recall, we were successful in getting
16 a commitment to this important requirement placed in
17 the DHS 2010 grant guidance. Grant awards have been
18 made. They were made over the summer, basically end
19 of July, beginning of August, so our clock is ticking.

20 As you may recall, the grant guidance
21 indicates that the privacy policy must be completed
22 and reviewed and confirmed by my office that it's at

1 least as comprehensive as the privacy guidelines in
2 the information sharing guidance within six months of
3 receiving the grant funding, so the clock is
4 definitely ticking. Our goal is 100 percent
5 compliance, and we'll do everything we can to help the
6 centers get their policies in place.

7 To date, we have reviewed and approved 25
8 Fusion Centers policies, and we're in the process -- I
9 believe we have four more in my office for review. In
10 case you think 25 of 72 doesn't sound very impressive,
11 please keep in mind that the Privacy Office review is
12 only at the end of a very robust Technical Assistance
13 Program managed by the Department of Justice, and in
14 fact we are not editing the policies per se, we're
15 confirming the compliance because of federalism, quite
16 frankly.

17 So many more policies are in advanced stages
18 of the review pipeline, and we're expecting more and
19 more to arrive for the final review in the coming
20 weeks and months. We anticipate that the number will
21 wane you know in February, March and April, so we
22 should be able to meet all of those timing

1 requirements, and I've dedicated the staff to make
2 sure that that takes place.

3 The Fusion Center support in general, and
4 the training and the privacy policy review
5 specifically, were the subject of an extensive review
6 of the Fusion Center program at large conducted by the
7 Government Accountability Office.

8 While the results are still in draft, it's
9 good to have an outside perspective on our activities,
10 and we look forward to any findings or recommendations
11 they may have for us. While I'm on the subject of
12 GAO, let me say we're nearly complete in closing out
13 the recommendations made to us in GAO Report 07-522.

14 There, as some members of the Committee may
15 recall, GAO examined the operations of the DHS Privacy
16 Office and made four recommendations to improve
17 operations related to the designation of component
18 privacy officers, done; conducting a required biannual
19 SORN review, done; the timeliness of our annual report
20 -- as you can see, no problems there; and how privacy
21 incidents are being treated in the annual report.

22 We've concurred with all four of the GAO

1 recommendations and have been working hard to
2 implement them ever since. GAO is conducting a
3 periodic follow-up, and I'm confident they will agree
4 as will the Committee, that we have taken steps to
5 satisfy each of the recommendations thoroughly.

6 We also continue to be extraordinarily busy
7 on the international front. John Kropf, who is my
8 Senior Advisor on international privacy policy in
9 addition to being my deputy, the International Privacy
10 Policy Directors and I, coordinated with the DHS
11 Office of General Counsel and Office of International
12 Affairs, Departments of State and Justice, on current
13 privacy issues related to U.S./EU information sharing
14 agreements in general, on a binding U.S./EU agreement
15 based on the High Level Contact Group principles, and
16 our redress options for non-U.S. persons.

17 The International Privacy Policy Group
18 regularly participates in U.S., interagency and
19 multilateral planning meetings of the OECD working
20 party on information, security and privacy.
21 Discussions are ongoing on the draft OECD privacy
22 guidelines anniversary report, as is planning for the

1 October OECD conference in Jerusalem.

2 As I mentioned to you earlier this year, our
3 office is sponsoring a study of the public sector
4 implementation of OECD principle privacy guidelines.
5 We expect to issue a final report in December. And we
6 continue to develop our privacy training for DHS
7 international liaisons and attaches.

8 During the last three months, IPP has met
9 with training and international staff at DHS
10 components with the largest international presence to
11 determine the best means of delivering the training.
12 They're currently working on online training options
13 and hard copy takeaways and how to best incorporate
14 this material in existing U.S.-based training
15 programs.

16 We had a great deal, many, many trips --
17 probably too many to enumerate -- but I just wanted to
18 highlight that the Privacy Office continues its
19 international outreach, both with people coming to the
20 United States as well as necessary trips abroad,
21 particularly if we can leverage some other elements.

22 Just last week I joined the Department of

1 Justice's Chief Privacy and Civil Liberties Officer,
2 to lead a discussion on data privacy and PNR during a
3 seminar for U.S. law enforcement attaches and public
4 affairs and global affairs officers posted in Europe
5 that was sponsored by the U.S. Mission to the European
6 Union.

7 As you can see, we continue to promote and
8 push out DHS privacy compliance practices to an
9 international audience in many ways and to increase
10 transparency and to promote best practices, which are
11 my goals, whether it be within the Department or
12 throughout the privacy community.

13 With that said, Mr. Chairman, that is my
14 report.

15 MR. PURCELL: Thank you, Mary Ellen, very
16 much. It's very good.

17 There's a couple of things that I wanted to
18 follow up on that we didn't talk about today. One
19 was, I wanted to make sure the Committee's aware of
20 your outreach to the advocacy groups. Could you
21 comment on the meetings you've had with them and the
22 most recent meeting?

1 MS. CALLAHAN: Sure, I'd be happy to. Thank
2 you. As you know, I've established quarterly meetings
3 with the advocacy groups entitled Privacy Information
4 for Advocates, so it's the PIA meeting. Because we
5 love acronyms in the federal government. I thought of
6 that one myself. I know you're probably surprised.

7 So we have these quarterly sessions that are
8 scheduled. I kind of arbitrarily have picked the
9 third Friday of the first month of every quarter. So
10 we actually had our last one just on the 17th of
11 September.

12 The third Friday does not overlap with the
13 Privacy Coalition's meetings, which are the fourth
14 Friday of every month, right Jim? I think they're
15 every month. Privacy Coalition; do you know?

16 MR. HARPER: I don't.

17 MS. CALLAHAN: You don't know.

18 MR. HARPER: I don't know.

19 MS. CALLAHAN: So it was intended to not
20 overlap it. So those have been very useful and very
21 successful. We have had two since our last meeting.
22 The one in June was devoted to advanced imaging

1 technology, and to discussing the issues associated
2 therein.

3 So in addition to inviting every privacy
4 advocate that we knew and that we have an e-mail
5 address for, we also invited people from the Civil
6 Rights Civil Liberties community, or areas who have
7 issues or questions about impact related to religious
8 practices, using the AIT machines, and also travel
9 advocates.

10 And so we had a full house in June to
11 discuss these issues, and then we had a follow-up
12 demonstration for all of those who were interested in
13 seeing the AIT machine and talking about the
14 underlying privacy protections, the built-in
15 protections.

16 The PIA that took place last week was a
17 general one, where we talked about a variety of issues
18 that we're facing in the Department, and that was when
19 I was able to unveil the Annual Report. In addition
20 to those activities, kind of more comprehensively with
21 the PIA, we also in July spoke to the Privacy
22 Coalition on cybersecurity implementation.

1 And yesterday I met with the ACLU on --
2 there is a pilot in Boston and in Las Vegas associated
3 with having a standardized pat-down procedure that the
4 Transportation Security Administration has
5 implemented. And so we talked about those issues.

6 And so I continue to try to engage on
7 whatever issues people want to discuss in terms of
8 outreach, advocacy or questions about DHS programs.

9 MR. PURCELL: Excellent. The other question
10 I had, Mary Ellen, is vastly more self-serving. I'm
11 very curious to make sure that we understand how the
12 Committee's been able to support and affect the privacy
13 Office.

14 So we recently completed two papers, one on
15 information sharing and access agreements, another on
16 software as a service and the implementation there,
17 some guidelines. And I was wondering if you'd be able
18 to inform the Committee as to the effect of those, how
19 they've made any substantial effect on your
20 operations.

21 MS. CALLAHAN: Yeah, no, absolutely. Thank
22 you for that question, and that is something that I

1 intend to impalement or to make sure we do give you
2 guys feedback on how things are implemented.

3 With regard to the information sharing
4 implementation, I believe that my colleague, Helen
5 Foster, did present in May to kind of talk about how
6 we have implemented that.

7 With regard to the two papers that you guys
8 approved, which also I think was in May or March on
9 the system oriented architecture and on the redress --
10 those were the two that were both signed out the same
11 day.

12 The system oriented architecture, the
13 Privacy Technology Committee Group, together with
14 Compliance, are working on doing standardized Privacy
15 Impact Assessments, to make sure that those are
16 integrated and to make sure that we're implementing
17 the technology. And I think we'll probably have
18 something on that in December for you.

19 And then with regard to redress, as you know
20 that's a very important issue for us. The paper that
21 you guys produced was shared with the Secretary, with
22 her special counsel, who is working on redress issues,

1 and it was the basis for several of the elements that
2 are being implemented on several Redress Programs and
3 communication aspects of those Redress Programs that
4 are not yet final on an interagency level.

5 So that's probably as specific as I can get
6 on that. But that certainly was absolutely a
7 cornerstone for our addressing those issues.

8 MR. PURCELL: Do you expect the redress -- a
9 Fuller briefing will be available in December on that?

10 MS. CALLAHAN: Yes, I think so. I think it
11 is. We have to figure out what we want to say and not
12 say on certain things, but I think we can, and we may
13 have other parts of the Department do those briefings.

14 MR. PURCELL: Thank you very much.

15 MS. CALLAHAN: Thank you for the support.

16 MR. PURCELL: Sure. Turning to the
17 Committee now, first I'll turn to Joan, please.

18 MS. MCNABB: Thanks. Do we need this?

19 MS. CALLAHAN: Yes.

20 MS. MCNABB: Okay. I'm interested in
21 knowing how -- first of all, do your FOIA officers
22 handle Privacy Act requests?

1 MS. CALLAHAN: Yes.

2 MS. MCNABB: And what are some of the
3 differences between the way they respond to those and
4 to FOIA requests?

5 MS. CALLAHAN: So the -- if you're asking for
6 a first party request for information, we generally
7 call them a FOIA request even though they are a
8 Privacy Act request. Privacy Act and FOIA have
9 overlapping but sometimes different exemptions that
10 you can take.

11 As you know, the Department of Homeland
12 Security has a mixed systems policy which says that
13 even though the Privacy Act on its face only applies
14 to U.S. citizens and legal permanent residents, from
15 an administrative perspective we're going to treat
16 everybody the same.

17 And so therefore, we apply Privacy Act and
18 Freedom of Information Act exemptions to each of the
19 documents. It is most clearly at USCIS where they have
20 the most first party number of requests, but the idea
21 is to make sure that the broadest exemptions that we
22 can apply are indeed applied.

1 There may be some changes in our numbers as
2 we do change some elements. The Attorney General has
3 asked that we migrate and split out the Privacy Act
4 requests versus the Freedom of Information Act
5 requests. And so the numbers that I quoted to you may
6 change and morph, but I think the impact will be --
7 the total number of FOIA and Privacy Act requests will
8 be six figures for the Department for the foreseeable
9 future.

10 MS. MCNABB: Do you have a sense of sort of
11 the proportions of each in that?

12 MS. CALLAHAN: So USCIS is about two-thirds
13 to 70 percent of the requests that DHS receives.

14 MS. MCNABB: I mean and most of them --

15 MS. CALLAHAN: And of those I would probably
16 say --

17 MS. MCNABB: -- are privacy?

18 MS. CALLAHAN: I would probably say 70
19 percent of those are Privacy Act requests. And that
20 may be a low estimate, but that's probably right.

21 And one of the other things that we have,
22 the Disclosure and FOIA Group are to focus on is to

1 make sure, Joan, that we are consistent in how we
2 implement the Privacy Act and the Freedom of
3 Information Act exemptions, and that is something
4 we're going to focus on in FY2011.

5 And in fact let me take an opportunity to
6 mention that I believe in December of 2010, so coming
7 up, we're going to have our first Department-wide FOIA
8 training. And so it's going to be training that's run
9 by my Disclosure and FOIA Group.

10 They're doing a great job in preparing the
11 materials, and I have it as a bookend to the privacy
12 training which always takes place in June. And so
13 between the two, we will I think do a great job of
14 systematizing and leveraging best practices across the
15 Department.

16 MS. MCNABB: Thank you.

17 MR. PURCELL: Thank you. Lance.

18 MR. LANCE HOFFMAN: Good morning and thank
19 you for that good report. Especially I liked the fact
20 that the grant guidance for Fusion Centers is
21 seemingly moving along. With respect to that, how are
22 we on grant guidance for other elements, non-fusion

1 centers? What's going on if anything, in that regard?

2 MS. CALLAHAN: I'm shocked, shocked you
3 asked that question, Lance. I think you've asked that
4 question every committee meeting.

5 MS. MCNABB: Or I have.

6 MS. CALLAHAN: Oh, yeah, exactly, one of the
7 two of you have.

8 I can say that it's going very well. The
9 grant guidance -- we are in a continuing resolution,
10 or will be in a continuing resolution starting October
11 1st; therefore the grant guidance will not be issued
12 until we move into a new fiscal year.

13 We have had -- I don't want to foreshadow it
14 too much -- we have had useful conversations with the
15 grant office at FEMA, and they are supportive. We
16 hope that there will be language in the FEMA grant
17 guidance, if indeed we ever get out of a continuing
18 resolution.

19 Thank you for your continued questions on
20 these issues.

21 MR. PURCELL: David.

22 MR. DAVID HOFFMAN: Mary Ellen, Thanks for

1 being here today. The U.S. Senate's been taking up as
2 a top priority the potential for passing cybersecurity
3 legislation. Some of the draft bills that have been
4 out there would create new organizations in DHS and
5 also create responsibilities for DHS for supervising
6 the cybersecurity of the national information
7 infrastructure and covered critical infrastructure.

8 I'm wondering to what degree has your office
9 been involved in assessing what the privacy
10 implications of that legislation would be?

11 MS. CALLAHAN: Obviously whatever that our
12 U.S. Congress decides to do we fully support and will
13 implement appropriately.

14 With that said, we certainly have had -- we
15 certainly have been involved in making sure that
16 privacy protections are implemented in whatever
17 oversight elements that there are that could come out
18 of, whether it's new legislation or new cyber
19 opportunities themselves.

20 I think that's all I can say on that, David.

21 MR. PURCELL: Ramon, please.

22 MR. BARQUIN: First of all, Mary Ellen,

1 very, very good update here. Just two quick
2 questions. One is, there is a lot that's being pushed
3 by the current Administration under this general
4 umbrella of open government. And most of what I
5 understand you have done deals with the actual putting
6 up of certain data sets.

7 But there's another part of open government
8 that is sort of rampant, both on the positive and
9 potential for some problems, and that's the use of
10 social media. And I'd like to just hear from you
11 what, if anything, has been happening at DHS, and how
12 is your office dealing with some of that.

13 The other very, very quick question that I
14 have to do with -- we've heard a lot about some of the
15 travails or problems that the Googles of the world
16 have been having with China or whatever, and privacy
17 is always somewhere in the middle of that. And I know
18 it's tangential to our internal mission, but the
19 question is, are we tracking that and are there
20 lessons learned for us in that area?

21 MS. CALLAHAN: Thank you very much, Ramon.
22 And let me clarify -- let me kind of break down what

1 my office is doing on the open government stuff
2 specifically, and I'll of course address the social
3 media element, which in fact you're going to hear more
4 about in December.

5 But I'm very thrilled, glad that you asked
6 that question. So with regard to open government
7 there are many elements in terms of trying to disclose
8 and trying to be more transparent and to operate.
9 You mentioned the data sets, which of course are
10 important.

11 And our office is involved to make sure that
12 there's not an inadvertent or inappropriate disclosure
13 of personal information through the data sets. That's
14 what the Privacy Technology Group does as part of its
15 review. That's only one element.

16 There are several elements on the FOIA side,
17 which again are part of the transparency in open
18 government. The Office of Management and Budget had
19 recommended, for example, a 10 percent reduction in
20 backlog. I mentioned that DHS had established a
21 higher, 15 percent backlog which we, knock on wood,
22 will meet again, which I would not have told you in

1 July we were going to meet just because of this
2 increased volume.

3 And then we also have the Pro-Active
4 Disclosure directive that I have issued to the
5 Department to make sure that people are -- FOIA
6 officers in particular but also public affairs
7 officers are proactively disclosing information that
8 can be disclosed.

9 Not asking them to circumvent Freedom of
10 Information Act, but instead to make sure that the
11 information that can be disclosed is disclosed,
12 hopefully in a proactive fashion. And we've put up a
13 couple to several thousand different documents
14 associated with proactive disclosure.

15 So those are the types of elements that my
16 -- and then we also are of course involved in the
17 policy and the development side of the open government
18 plan, and that's led by my special assistant Lynn
19 Parker, and how to implement that in a privacy
20 protective way. There's a lot of also kind of
21 financial stuff and others we're involved in, but my
22 office isn't leading.

1 With regard to social media, we're of course
2 very involved. And in fact, on I think it was August
3 25th, we released a Department-wide Privacy Impact
4 Assessment on use of social media and specifically the
5 standards that need to be met in terms of how to
6 disclose that you're a DHS entity, how to friend and
7 not friend people, what to disclose, what information
8 to collect and how to do so in a transparent way.

9 Going forward, if there are new technologies
10 or new applications or new uses of social media, then
11 those applications will not be turned on until we
12 approve it, to make sure that again, we're having the
13 same privacy protections across the board, but that we
14 are also making sure that -- it's more efficient for
15 everybody to go and say, okay, this is what we're
16 going to do, this, this, this and this, and to make
17 sure that the disclosures are indeed the same. And so
18 I think it will be more efficient at the end of the
19 day and also I think a better privacy protection with
20 regard to that.

21 The Associate Director for Compliance, Eric
22 Leckey, is going to talk about our social media

1 initiatives in December. We were going to have him
2 talk now, but I was like, there's too much going on.
3 So he'll talk about that in December, but thank you
4 for that question.

5 With regard to international activities in
6 an online capacity, I think we can say that it
7 certainly is something that's been in the public
8 domain, and it is a concern in terms of how to
9 implement, and I think that the public conversation
10 about that is an appropriate one. And that's as far
11 as I'll go on that. Thanks.

12 MR. PURCELL: Lisa, please.

13 MS. SOTTO: Thank you, Richard, and thank
14 you, Mary Ellen.

15 Question for you about your international
16 discussions. You've been globetrotting recently. I'm
17 interested in the tenor of those meetings. The tenor
18 in the past has been a little bit testy, I would say,
19 and I'm wondering if that's been mitigated at all, and
20 whether the Europeans are still harping on the fact
21 that we don't have an independent privacy office here.

22 Is that still an issue for them?

1 MS. CALLAHAN: So I think the tenor actually
2 is quite good, and I think -- when I took this job I
3 thought it was a domestic job. But I actually think
4 you know that the world is getting much smaller and
5 the international impacts are getting greater. And so
6 the Secretary's asked me to devote a certain amount of
7 time to my trips to -- I've taken nine trips to Europe
8 and one to Canada, and I'll take another one to Canada
9 in November, I think.

10 And so the -- with that said, the
11 Secretary's asked me to devote a certain amount of my
12 time to that. And on each trip, on each visit, and
13 each time when we go and meet with people in the
14 United States, by and large it's been very productive
15 and very useful conversation.

16 You know we don't has a one-sentence word of
17 -- we can't say, we have a 1995 directive on data
18 protection, and it says X, and we have Article 8 of
19 the Charter of Fundamental Rights and it says Y. We
20 don't have that. We have a pretty nuanced process
21 that you guys are intimately involved in, understand,
22 but it's not a sound bite.

1 And so we've spent a lot of time, myself,
2 John and the International Privacy Policy Directors,
3 explaining this process. And I think it's been very
4 useful. And each time I go I feel like I've made
5 headway. What's frustrating is that apparently I have
6 to make headway with 500 million Europeans. Because I
7 have to talk to each one of them about it is the only
8 way I feel like I've made some progress.

9 The European Union is our strongest ally,
10 and they are our strong supporters. With that said,
11 the focus on specifically having an independent data
12 protection director/commissioner type of position, was
13 something that came up a lot, as was judicial redress.

14 And we talked about all the different
15 elements and explained that with regard to the
16 multitude of privacy laws that are in the United
17 States that impact the public sector, the only kind of
18 non-overlap area where the Privacy Act applies but no
19 other law applies, would be a circumstance where
20 somebody sought access -- so a non-U.S. person sought
21 access to their records, accessed their records,
22 received them, found that there was a mistake, wrote

1 to the Department, in this case wrote to me as FOIA
2 Officer, asked for the correction, and I denied it as
3 an administrative function.

4 And then they sought to seek judicial review
5 of that decision where I say, no, Lisa Sotto, I'm not
6 going to change your gender from male to female. I'm
7 going to keep it as male in our documents, right.

8 Now, of course, from an administrative
9 perspective, you know one of the Fair Information
10 Practice Principles is data quality and integrity, so
11 you want to have the best record that there could be.

12 And so I just can't imagine that if somebody
13 came to us, demonstrated there was a mistake and ask
14 that it be corrected, if there was basis to make that
15 change, whether you be a non-U.S. person or a U.S.
16 person, we would of course make the change.

17 And in fact, we get a handful of those types
18 of requests a year, and we don't know if they're U.S.
19 persons or non-U.S. persons. But the point is, if I
20 had denied it on an administrative level, there
21 wouldn't have been an ability to appeal, where under
22 the Privacy Act there would be this ability.

1 That seems like a very narrow non-
2 overlapping element of the Venn Diagram, and that, and
3 maybe even be a null set at the end of the day, in
4 terms of how it applies, because other than that
5 element, the rights of European citizens are the same
6 as U.S. citizens across the board.

7 And so trying to explain that has been
8 interesting, but at the same time, the -- you know
9 we're looking to try to make the option of a judicial
10 redress more concrete, so we're also looking at that.

11 Even trying to explain that non-overlapping Venn
12 Diagram, that takes too long. So we are looking at
13 options to make it more concrete, but also consistent
14 with U.S. law.

15 MR. PURCELL: Thank you. Neville, please.

16 MR. PATTERSON: Thank you. Mary Ellen, you
17 mentioned some private incident review dated in June
18 from the February to March area. Can you give us any
19 understanding of the nature and severity of these
20 privacy incidents and any corrective actions that your
21 office is involved in?

22 MS. CALLAHAN: Yeah. No, thanks, Neville.

1 We did the review in the Spring and then we also did
2 the kind of annual review. And as we talked about in
3 I think it was December, you know when you have
4 increases in training, you also have increases in
5 numbers, which were definitely demonstrated.

6 ICE was the person this time, when it was
7 USCIS last year for the fiscal year. With that said,
8 the severity had decreased, as we had suspected. One
9 thing we were not able to capture, and this goes to
10 one of the questions Kirk asked us in December, was
11 the actual raw number of persons impacted.

12 And I've talked to the CIO and to the EOC,
13 which are the people who receive the complaints and
14 with whom we work a lot to try to get a better way of
15 calculating that for next fiscal year. But you can
16 tell in terms of the severity and to the dialog, what
17 the elements are.

18 We had an increase in portable devices,
19 which again is not surprising, as they have increased,
20 as well as you know, kind of minor transgressions.
21 But the portable devices and I would say, e-mailing
22 unsecure or unencrypted or to unsecure e-mail

1 addresses were kind of the themes that we had.

2 And as I said, we do have this ongoing
3 investigation associated with several components where
4 there was a breach by a contractor that you'll hear
5 more about in December. But I think that we're going
6 to have good policy recommendations to come out of
7 that, and that will be one of my reports pursuant to
8 my investigatory authority.

9 MR. PURCELL: And John Sabo and then Renard
10 after him.

11 MR. SABO: Thank you. Thanks, Mary Ellen.

12 Everybody's been talking -- my question was
13 on international, and you talked about best practices
14 and you've answered a number of questions on that.

15 It would seem to me that in some senses,
16 your office is, with FTC I suppose, are the two U.S.
17 entities that are interfacing with the Euro -- you
18 know, data protection commissioners in Europe and at
19 the ECC level as well as the member state level.

20 And I'm wondering, a friend of mine just
21 returned from a cruise to Japan. And apparently Japan
22 and perhaps other countries are now adopting some U.S.

1 practices to get into the country off the ship. You
2 had to do a -- I'm not sure if it was a 5 print or a
3 10 print entry.

4 And that leads me to think, this is going to
5 proliferate, and in the absence of a designated data
6 protection officer for the United States, are you
7 looking at or -- and I know this is not your primary
8 role, but in effect best practices, bilateral
9 practices, practices that are adopted internationally,
10 that would help American citizens and the protection
11 of their privacy in other regimes that are equal to
12 some of the protections that you've help build for
13 DHS, probably would help build an international
14 consensus.

15 And you know who is responsible for doing
16 that, and is that an ancillary value of what you see
17 you're doing in the international space? I guess I'm
18 just asking generally if you see you can help
19 influence from the practices perspective based on some
20 of the things you put into place in DHS?

21 MS. CALLAHAN: Thank you, John, and we
22 certainly are willing to share our best practices in

1 terms of implementation. As I said, the IPP has met
2 with a lot of people. John Kropf has traveled to a
3 couple of different biometric conferences to talk
4 about the implementation, and of course, US-VISIT is
5 quite active in international discussions, both at the
6 director level but also obviously with Paul Hasson,
7 the US-VISIT Privacy Officer.

8 And so we're certainly willing to engage on
9 these issues and on kind of best practices at large.
10 It's an interesting phenomenon having just come back
11 from Europe, where as you guys know -- you know me by
12 now. I'm very much about getting the job done, and
13 application and making sure that the impact is
14 implemented and is set throughout.

15 I have not yet gotten a clear sense of how
16 the European Data Protection authorities implement
17 privacy protections. They are very good at
18 discussing, particularly Article XIII of the Charter
19 of Fundamental Rights and the '95 Directive, but I'm
20 like, so how do you do it?

21 How do you operationalize it? How do you do
22 it every day? And I haven't gotten a sense of that.

1 And I would love to have that kind of dialog
2 concretely, right, and that's a very European thing --
3 let's have a technical discussion with experts, is
4 what they always say -- of kind of how do you do it
5 day to day.

6 Whether it's on the biometric side or just
7 in general, public sector, privacy protections, and so
8 on, I'd be interested in that. But to the extent that
9 people do want to leverage what we've learned and the
10 privacy protections embedded therein, we welcome the
11 conversation.

12 MR. PURCELL: Renard.

13 MR. FRANCOIS: Thank you very much. I just
14 had a quick question about the Fusion Centers, and I
15 understand that there's been training that you all
16 have done and undertaken, and also, a review of the
17 privacy policies.

18 My question is, are there any plans to maybe
19 circle back at some point and audit the Fusion
20 Centers' practices to see whether they are consistent
21 with the training and also consistent with the privacy
22 practices, and if there are, would your office be

1 involved, or would that be something separate?

2 MS. CALLAHAN: Yes. But I think we have to
3 be sensitive here. So again we have federalism
4 elements here in terms of the U.S. government
5 surveying, auditing, reviewing a state or a city-run
6 entity. And I'm looking at Joan on this issue.

7 With that said, Renard, there are several
8 different things that I think would help ameliorate
9 your concerns. One is that there are Fusion Centers
10 reviewing Fusion Centers right now, and so they're
11 kind of doing a review of each other, so to speak,
12 using a template that we did have input into in terms
13 of making sure that privacy civil liberties and civil
14 rights protections are embedded within the process,
15 how are they implementing it and so on.

16 So the Fusion Centers are reviewing each
17 other, and we were part of the kind of design of that
18 review. We didn't write it, because that was a Fusion
19 Center organization opportunity, but we did make sure
20 that the kind of -- that the baseline capabilities
21 were identified in the implementation process. How
22 that review's going, I don't know, but I do know that

1 it is ongoing, and it's kind of making sure that these
2 Fusion Centers are standing up in the proper way.

3 Another way that we could do it is we are
4 going to circle back with the Privacy Officers. The
5 train the trainer process was again, an introductory
6 element into these Privacy Officers to make sure that
7 they had kind of the rudimentary skills, but they were
8 instructed to have their own privacy and civil
9 liberties training within six months. So there'll be
10 a circling back, together with the Office of Civil
11 Rights and Civil Liberties, to do that and seeing how
12 that implementation is going.

13 And then the third element is we of course,
14 are required to do a second Privacy Impact Assessment.

15 We did a first Privacy Impact Assessment before I
16 came on board in December of 2008, but we're required
17 by law to do a second one, and I think this one is
18 going to be more instead of kind of future-looking,
19 but also this will be, how are things going as they
20 stand right now.

21 So I think the PIA coupled with the internal
22 review and the experiences that we're learning through

1 the train-the-trainers and the in-person training,
2 will be useful to make sure that we fill in any
3 identified gaps.

4 MR. PURCELL: Mary Ellen, thank you very
5 much for your time today, and this update is very, very
6 helpful to us all. We appreciate it very, very much.

7 Thank you.

8 MS. CALLAHAN: Thank you for your time.

9 MR. PURCELL: Thank you very much.

10 Now, our next guest is Jamie Pressman.
11 We've cut seriously into Jamie's time, which we will
12 yield back to her. But I do apologize for keeping you
13 waiting. The opportunity to query Mary Ellen is
14 irresistible for all members of the Committee.

15 Ms. Pressman has joined the Privacy Office
16 last year as Associate Director of Privacy Compliance.

17 She's here today to brief us on the Privacy Office's
18 efforts to build more accountability into the DHS
19 Privacy Compliance process through a review process.

20 Prior to joining the Privacy Office, Jamie
21 was a member of the Federal Service as a Senior Consultants
22 with DeLoitte. She provided in that capacity contract

1 support to the Privacy Office on information sharing
2 issues. I think most of the Committee members recall
3 your contributions during that time, and we're very
4 welcome to see you again.

5 For the last what, six years, Ms. Pressman
6 has worked at the U.S. Government -- or from 2002 to
7 2008, apologies -- at the GAO. She was a Senior IT
8 Analyst, led government-wide and agency-wide, or
9 agency-specific reviews of programs focusing primarily
10 on privacy.

11 Ms. Pressman, thank you for joining us.
12 Please proceed.

13 STATEMENT OF JAMIE PRESSMAN, ASSOCIATE DIRECTOR,
14 PRIVACY COMPLIANCE, UNITED STATES DEPARTMENT OF
15 HOMELAND SECURITY

16 MS. PRESSMAN: Thank you. Good morning,
17 Chairman Purcell and members of the Committee. This
18 week actually marks my one-year anniversary in my
19 position here at the Privacy Office.

20 MR. PURCELL: Congratulations.

21 MS. PRESSMAN: And I'm excited to be here
22 today to talk about what I and my colleagues think

1 will be the next phase in building the privacy
2 compliance framework.

3 This morning I will provide an overview of
4 the need for compliance reviews, the planned scope of
5 the reviews, and a framework for guiding the
6 development and execution of the reviews by our office. I
7 also understand there's interest by the Committee in
8 this issue, so there will also be time for questions
9 at the end.

10 Privacy compliance is built into many
11 existing processes here at the Department in an effort
12 to get privacy in at the earliest stages of IT system
13 and program development. Over the years, the Privacy
14 Office has worked diligently with our partners in the
15 CIO's office to incorporate privacy requirements into
16 processes for IT system development, budget, rule
17 making, and the Paperwork Reduction Act.

18 By tying requirements such as the completion of
19 the privacy threshold analysis into these existing
20 processes, system developers and program managers are
21 better positioned to incorporate requirements at an
22 earlier stage of the development of these systems and

1 programs.

2 Through a more mature privacy compliance
3 framework and a growing network of component privacy
4 officers, we believe that the basic privacy compliance
5 requirements are fairly well understood at DHS. For
6 example, it's well understood that privacy
7 documentation, including the PIA and the SORN must be
8 complete before a technology or system deploys.

9 Anyone who's drafted a PIA or a SORN can
10 attest to the amount of work that goes into these
11 processes. Completion of the PIA itself is in
12 essence, a review of the program or the system through
13 the privacy lens.

14 And while programs must revisit their
15 documentation every three years or whenever a
16 significant change occurs, we in the compliance group
17 are looking for other avenues other than a
18 documentation refresh to make sure that programs are
19 accountable for what's stated in their documentation.

20 We also view the compliance reviews as the
21 next logical step in maturing the privacy compliance
22 framework. So the Privacy Compliance Review is an

1 extension of the Chief Privacy Officer's authority
2 under Section 222 of the Homeland Security Act, to
3 assure technologies sustain and do not erode
4 privacy protections.

5 This is consistent with the Privacy Office's
6 unique position as both an advisor and an oversight
7 body for the Department's privacy sensitive systems
8 and programs. The PCR is designed as a constructive
9 mechanism to improve a program's ability to comply
10 with assurances made in the documentation.

11 And I use the word proactive because I see
12 this as a key distinction with the role of our office
13 versus what an IG or GAO would do. GAO or the IG
14 would typically come in after the fact to review what
15 went wrong, and our goal here is to be proactive and
16 try to remediate any issues before they actually
17 become real issues.

18 The Privacy Office, under the leadership of
19 the compliance group, will initiate reviews at the
20 discretion of the Chief Privacy Officer, as well as
21 when an agreement obligates our office to conduct a
22 review of a program or a system to assess compliance.

1 For example, this office has periodically
2 conducted reviews of DHS's use of passenger name
3 records, and that was consistent with the terms of the
4 EU/U.S. PNR Agreement. We most recently conducted a
5 review update in February 2010, and we will continue
6 to do reviews of our use of PNR. But the privacy
7 compliance Review framework will also provide
8 opportunities for us to look at our use of information
9 through Memoranda of Understanding, Memoranda of
10 Agreement as well.

11 In addition, under the Chief Privacy
12 Officer's discretion, a review may be planned as part
13 of the development of a new program or system for
14 those that present unique privacy concerns or may
15 involve controversial issues that may heighten public
16 scrutiny.

17 An example, a most recent example of this,
18 is the review conducted on the Department's use of
19 social media by the Office of Operations, Coordination
20 and Planning. In this instance, the program prepared
21 a PIA to describe their planned use of social media
22 for monitoring during the 2010 Winter Olympics and the

1 Haiti earthquake. And the rules in the PIA actually
2 proactively included a provision for the compliance
3 group to verify adherence to the rules outlined in the
4 PIA.

5 We recently just concluded that review and
6 found that the program indeed did comply with
7 assurances made in the Privacy Impact Assessment. The
8 only shortcoming there was that they had not finalized
9 their NARA records retention schedule, but we'll be
10 following up with them later this fall to make sure
11 that that issue gets closed out.

12 That report was also made available on our
13 Privacy Office web site, I think just about two weeks
14 ago. Another opportunity for conducting a privacy
15 compliance review could be for a privacy incident,
16 which would be on an ad hoc basis, and we would
17 consult with our director of Privacy Incidents and
18 Inquiries.

19 Typically the composition of the review team
20 would be members of the compliance group, potentially
21 members of policy staff and also another key aspect is
22 involving the components privacy offices. That's very

1 important because they're even closer to the actual
2 program.

3 And the output of the privacy compliance
4 review, is consistent with our transparency goals.
5 Our intent is to publish the results of any review
6 that we do on our web site. We've done that for the
7 social media review. It was a very short review. It
8 was only six pages. PNR reviews have typically been a
9 little bit longer because the criteria that we're
10 reviewing are a little bit more extensive in that case.

11 So now that I've sort of given you an idea
12 of what we're looking at in terms of the scope of the
13 reviews, I want to talk about just the basic steps
14 from the design to the execution of the review.

15 So as Chairman Purcell mentioned, most of my
16 experience was with the U.S. Government Accountability
17 Office, so I'm a recovering auditor. And I actually
18 led a review of this office back in 2007, so I have a
19 very unique perspective into this office and also from
20 the auditor side. So that's really helped me out a
21 lot in this position.

22 So I definitely see the roles of the

1 Inspector General, GAO and the DHS Privacy Office as
2 all important, but they're distinct roles. And I
3 think here, the Privacy Office serves -- sort of it's
4 a hybrid of an oversight entity and an advisor, and I
5 think the Privacy Compliance Review is the perfect
6 combination of those things.

7 So the Privacy Compliance Review framework,
8 basically covers eight basic steps, from the design of
9 the review to execution to publication of the report.

10 So the first step, very basic. The team would
11 collect and review available background information.

12 This would mean going back, finding out,
13 reading through the SORN, the PIA, if there are MOUs
14 involved, if there are any IG reports out there, any
15 other publicly available reports. And then the second
16 step is critical, formulating your review objectives.

17 So with the Privacy Compliance Review,
18 typically your first objective and sometimes your only
19 objective is going to be assessing a program's
20 compliance with the current privacy documentation and
21 applicable DHS policies.

22 There may be cases, though, where you would

1 add an objective to the review, as we've done with our
2 EU/U.S. PNR Agreements, because you have a lot of
3 criteria within the Memorandum of Understanding that
4 you want to assess the compliance against. And also,
5 depending on the type of program and concerns raised,
6 the review may be a more holistic look at the
7 program's compliance with the Fair Information
8 Practice Principles.

9 So the third step, very important, is
10 actually notifying the program that the Privacy Office
11 is going to come in and conduct a review. This would
12 typically come from Mary Ellen and the director of
13 Privacy Compliance and would go directly to the
14 program principal, and would say, let them know about
15 the Privacy Office's intent to conduct the review,
16 some generic statements about what the privacy
17 compliance review entails, what its goals are, and
18 what the objectives of our review are.

19 In the interim, the team in step four would
20 be formulating the review questions and document
21 requests. In step two we talked about formulating
22 review objectives and your review questions, and your

1 documents requests really flow logically from what
2 your objectives are.

3 So if it's a strict privacy compliance
4 documentation review, you're going to go and review
5 the PIA and the SORN and see if there are any
6 outstanding issues, formulate questions that make sure
7 they're continuing to comply with those practices.
8 And also, interviews will be a main source for us,
9 determining the outcome of the review, but it's not
10 the only source. We also will be doing document
11 reviews.

12 We'll ask for standard operating procedures,
13 other policies so that if someone in an interview
14 makes reference to a standard operating procedure,
15 we're going to ask for that and we're going to go back
16 and we're going to analyze it. And if we have follow-
17 up questions, we'll follow up with the program on
18 that.

19 But the idea is that we want to formulate our
20 questions and document requests, we want to do that
21 before we actually sit down with the program. This is
22 another distinction I see between what the IG and GAO

1 due.

2 IG and GAO have a more extended time frame
3 to conduct their reviews. Often a design of a review
4 can take up to three months, where they're just
5 figuring out what it is they want to study, and there
6 are benefits to doing that, but here we really want a
7 more expedited process.

8 We want to make the best use of everyone's
9 time. We realize programs have competing priorities,
10 so we want to make this as easy as possible for
11 everybody. So by the time we go in for the
12 interviews, we have all of our questions and our
13 document requests, and that's not to say that we won't
14 have follow-up, because there will be follow-up.

15 Step six involves analyzing the
16 documentation and interviews and starting to document
17 your preliminary conclusions, and that typically will
18 be a written record of analysis. There would be
19 reviews by the Director of Privacy Compliance, likely
20 by Mary Ellen as well. And we want to get that step
21 completed before we go through and we actually review
22 and confirm our findings.

1 At that point we're starting to draft a
2 report, and once we're comfortable that our findings
3 and our recommendations are substantiated, we'll set
4 up a meeting with the program to go over what are our
5 findings and if there are any recommendations, what
6 those are, give them an opportunity to comment on it,
7 bring any new information to our attention, and then
8 once that's all complete, we will prepare and issue
9 our report and then post it on our web site.

10 So that concludes the eight steps. I'd be
11 happy to answer any questions about the steps or how
12 we're planning to use it.

13 MR. PURCELL: Thank you, Ms. Pressman. I
14 have one question. How often are you finding that
15 procedures are either not documented or poorly
16 documented? Is that part of your systematic findings?

17 MS. PRESSMAN: I think more so from my
18 perceptive as GAO, I would say that that is very often
19 the case, that people say, this is how I do it, but
20 when you ask for the documentation that supports that,
21 it's often not there.

22 Now, I have been surprised in a few other

1 meetings. We've been doing some meetings on
2 suspicious activity reporting. There have been some
3 programs that to my surprise, actually said that they
4 had some written standard operating procedures and had
5 provided that to us. So that was very welcome.

6 MR. PURCELL: Pleasantly surprised. Members
7 of the Committee, Kirk.

8 MR. HERATH: Thank you. Thanks, Jamie.
9 Just quickly. Obviously you're trying to peanut
10 butter yourself over a very large organization. How
11 do you choose the entities? Is it risk based? Is it
12 sort of whatever is on the front page of the news? Is
13 it both?

14 MS. PRESSMAN: I think it's a little bit of
15 both. This is a new process. I think it is
16 primarily --

17 MS. CALLAHAN: We're not impacted by the
18 news.

19 MS. PRESSMAN: Mary Ellen says we're not
20 impacted by the news --

21 MR. HERATH: Oh, okay.

22 MS. PRESSMAN: -- but sometimes things that

1 are brought up by the news are high risk as well for
2 the Department. I mean, the PNR issue gets brought up
3 in the press a lot, but we were already obligated to
4 conduct reviews on that. So that's something we're
5 already subscribed to.

6 Other issues, I mean we decided to do this
7 compliance review on social media because that's
8 really a new use. And so while we were comfortable
9 with the program doing the social media monitoring for
10 the purposes they'd set out, we wanted an opportunity
11 to go back and review and see that they were doing
12 things properly, was there anything that needs to be
13 changed in terms of policy and procedures.

14 And right now we're really just looking for
15 candidates for what other reviews, what we might want
16 to do. We might look to do something with a component
17 privacy office. Nothing concrete yet, but we've
18 talked with the US-VISIT Privacy Officer about
19 potentially doing some sort of compliance review later
20 next fiscal year.

21 MR. HERATH: Something I found useful of
22 trying to start doing this ten years ago, we started

1 out assessing, finding that the policies and the
2 procedures were literally non-existent. So we
3 actually went back, and as sort of a preparation, we
4 spent several years working with all of our business
5 units, actually creating sort of model policies,
6 procedures, sort of figuring out what they did.

7 So we spent a lot of time in the advisory
8 role, just helping them help themselves and map all
9 the things that you're going to end up coming back and
10 looking at, so that when you do your assessment,
11 everything is in place.

12 And it has sort of a dual role. It has an
13 education awareness impact as well. So that's
14 something you might want to -- if you do find areas
15 that are just not doing as well as others, you might
16 want to spend some time just getting them prepared.

17 MS. PRESSMAN: Okay.

18 MR. PURCELL: Thank you. Charles.

19 MR. PALMER: Yes, thank you for your
20 comments. When doing security assessments, we found
21 over the years, you're trying to measure something and
22 the fact that you're trying to measure something often

1 modifies what you're trying to measure. This is not
2 surprising.

3 How much warning do the programs get, and do
4 you ever do this assessment without such warning?

5 MS. PRESSMAN: Well, this is really a new
6 process, so I can't think of any instance where we've
7 done it without warning. The PNR instance, it was in
8 the Memorandum of Understanding that this would occur,
9 so the program knew that it was coming.

10 In the case of the social media review, it
11 was built into the Privacy Impact Assessment itself.
12 So the program knew going in that we're signing up to
13 this particular use, but know that the Privacy Office
14 will be coming in to review your program later on.

15 In terms of new programs that we might look
16 at, we haven't really thought about how much notice to
17 give. The idea is that when we do notify them, we
18 know exactly what it is we're going to be looking for,
19 and they'll know what to expect. I hope that helps.

20 MR. PURCELL: Charles, do you have a -- do
21 you have -- in your experience, what do you find in
22 terms of prior notice?

1 MR. PALMER: Well, what you don't want is to
2 tell them, okay, we're coming and then have them run
3 down the hall in front of you locking the doors. And
4 you know there's a fine line between, well, that's not
5 fair or a valid, true assessment. And perhaps a
6 mixture is the right answer.

7 MS. CALLAHAN: So, I completely agree,
8 Charles. With that said, given that we have public
9 accountability, all of these components should
10 anticipate that we're coming.

11 And to a certain extent Jamie gives a little
12 bit of a preview on these things, but it seems to me
13 that if we go and say, October 1st, hey, CBP -- is
14 Larry in the room yet -- hey, CBP, we're going to
15 investigate X.

16 He's not going to be able to make any
17 changes you know in terms of making sure the privacy
18 protections are built in. There may not be anything
19 as Kirk says, but at the same time, I think we're
20 going to have an accurate snapshot of what we're
21 looking for.

22 MR. HERATH: I think so. I don't think

1 that's -- the role's not to play gotcha, right.

2 MR. PURCELL: No, not at all.

3 MS. PRESSMAN: That's it exactly. It's a
4 proactive feel.

5 MR. HERATH: You really do -- you're a
6 completely different role in your internal audits or
7 your IG, as you said, completely different role. And
8 in a way you're partnering with them, and you're
9 helping them help you, right.

10 Because at the end of the day, if they're
11 bad, you're bad, right. It means that you haven't
12 done your job in preparing them and preparing the
13 groundwork, educating, getting the policies and
14 procedures and the culture in place to do this. So
15 it's really an assessment of the Privacy Office as
16 much as anything at the end of the day.

17 MS. PRESSMAN: That's true.

18 MR. PURCELL: Thank you. Mr. Sabo.

19 MR. SABO: Oh, thanks. Just a quick
20 question. How proactive is your mission in terms of
21 compliance? In other words, is it just the reviews
22 and the audits and the post analysis that you're

1 required to do versus working with other components to
2 say, all right, we need active monitoring of X in the
3 system so that we can have automated reports generated
4 on an ongoing basis so we can review those.

5 In other words, a big move now in technology
6 is towards real time monitoring, real time analysis,
7 heuristics, a whole bunch of things that are now
8 allowing you, and I think from a security perspective
9 the State is very active in this in terms of its FISMA
10 active reporting.

11 So I guess the question is, is that a role
12 for your office where you take a look at the systems
13 that are in place, the reporting that is built into
14 them versus what you have to do in looking at
15 documentation and then advise to embed automated
16 reporting, to the extent it's practical into these
17 systems. Is that part of your role, or is that not
18 part of your role?

19 MS. PRESSMAN: Well, I think the information
20 security side right now is a little more well equipped
21 for continuous monitoring. I know that OMB FISMA
22 reporting this year, one of the metrics is on

1 continuous monitoring, and that metric does not at
2 this time apply for privacy. I'd be interested to
3 hear if there are tools out there available for
4 continuous monitoring.

5 I mean, our compliance framework in itself,
6 we do review -- you know the PIA expires after three
7 years. Your PTA expires after three years or if the
8 system has undergone a major change. System of Records
9 Notices are reviewed every two years, but in terms of
10 continuous monitoring, we haven't gotten to that stage
11 yet.

12 MR. SABO: I just make a comment you know
13 that a lot of -- and this has been a -- Mary Ellen
14 knows it's been a mantra of mine for a long time, that
15 the industry builds technologies or uses technologies
16 and builds solutions based on requirements. And it
17 seems to me that continuous monitoring, as applicable
18 to privacy, is an area where regulators and agencies
19 can say, we need these tools and then turn to industry to
20 build on it.

21 I just think in security you've seen that,
22 especially as you move into this online environment,

1 and I think there could be parts of the privacy
2 requirements that you have that could equally lead to
3 some form of more active monitoring in a whole bunch
4 of areas. And the standards community is a good place
5 to look to begin building standards but there's got to
6 be an impetus to do that.

7 It may not be your primary role now, but it
8 could be a valuable addition to the arsenal at some
9 point in the future, especially as you move into cloud
10 computing, moving into very distributed systems. It's
11 going to be virtually impossible to do detailed
12 assessments without a lot of data. So just a comment.

13 MS. CALLAHAN: John, this is Mary Ellen, and
14 I would say that it would be great if we were able to
15 do it. I think what Jamie's talking about in terms of
16 these proactive reviews are probably the first time
17 within the federal government that these types of
18 things are done.

19 And so I think we've got to go incrementally
20 here. I'm not saying that your goal isn't a good one.

21 We'd have to make sure that we go in stages, and of
22 course to have kind of continuous monitoring, even if

1 it's on a technological basis, would require a pretty
2 significant contribution. And my office certainly
3 can't support it. We're willing to support this and
4 Jamie's leadership on this, which I think is very
5 useful. But continuous monitoring is not foreseen in
6 my budget at this point.

7 MR. PURCELL: I think the conversation is
8 excellent if we reflect earlier in the conversation
9 that we had, two of the vulnerabilities that you
10 mentioned, are e-mail, unsecured e-mail and mobile
11 devices.

12 Those are two areas where I think the IT
13 department could actually be very helpful in creating
14 some -- if not continuous monitoring, at least some
15 spot monitoring for an ongoing compliance. Because
16 those areas are in continuous use, as well as if
17 there's a failure in any of those areas, that failure
18 can be rather dramatic, because you may not catch it
19 for quite some time. So that kind of monitoring may
20 be valuable.

21 MR. SABO: I just want to clarify. I wasn't
22 implying that you need to go out and -- that your

1 office needs to go out and buy something. I was
2 saying, as you build, as you input into system
3 requirements for the systems that are being built in
4 the future, to the extent that you, as a compliance
5 officer, would look to want to have certain kind of
6 reporting, those could be embedded. That's all it is.

7 MR. PURCELL: Right, that would be helpful.

8 Turning to Ramon, please.

9 MR. BARQUIN: Jamie, one of the areas that
10 falls under your overall privacy compliance ties to
11 the computer matching agreements. As my old Senator,
12 "Mac" Mathias, was -- but if I remember correctly, it
13 applied primarily where individuals were -- where
14 you're looking for eligibility for benefits.

15 And the question is, is there CMA
16 application and hence the need for compliance on, when
17 you're trying to do computer matching primarily for
18 you know, counter terrorist or other type of
19 activities. And tied to that, something very near and
20 dear to certainly our hearts in this Committee is, I
21 know that there is a Data Integrity Board, that is in
22 theory, I know, attached to the CMA. And the question

1 is, what is this Board doing if anything, aside from
2 CMAs and DHS?

3 MS. CALLAHAN: The Data Integrity Board is
4 being reconstituted to make it more effective. And
5 Mr. Leckey can speak to that in December as well.

6 MS. PRESSMAN: But we do still process
7 computer matching agreements. I think we did about
8 four this fiscal year.

9 MR. BARQUIN: And are they exclusively
10 related to this issue of eligibility for benefits, or
11 is it other applications?

12 MS. PRESSMAN: Right, that's what the
13 Computer Matching Agreements are for. It's only when
14 it's for a benefit where basically there's money
15 exchanged. I don't have the technical definition in
16 front of me, but there are not many within the
17 Department.

18 MS. SABO: Okay.

19 MR. PURCELL: And thank you for the humorous
20 aside about reconstituting the Data Integrity Board.
21 Renard.

22 MR. FRANCOIS: Thank you for your time.

1 Just two quick questions. The first was -- and I'm
2 not sure if you touched on it, it's about -- I'd love to
3 hear a little bit more about accountability that you
4 have after you've conducted a review of processes and
5 procedures and issued a final report.

6 If you make recommendations, how are those
7 followed up on? And if they're not followed up on,
8 how do you hold those component organizations
9 accountable for implementing those?

10 And the second question relates to, I know
11 this is a relatively new process, but whether you're
12 seeing certain trends in your audits and whether your
13 group is working with the training and education group
14 to develop more refined training that can be pushed
15 down to the components that relate to the issues that
16 might be coming?

17 MS. PRESSMAN: Okay. So with your first
18 question about recommendations, absolutely, that's one
19 of the goals in any review is, if you find any
20 weaknesses, we're going to issue a recommendation.
21 And we will be following up, especially if we find a
22 deficiency in their Privacy Compliance documentation,

1 that the recommendation would be in the report and we
2 would probably include a provision directly in the
3 report that says, we'll be following up with you in
4 three months to follow up on the status of the
5 recommendation.

6 And so far, with the one Privacy Compliance
7 Review that we did for social media, the one
8 outstanding issue -- as I understand, I think they've
9 already closed it out but we're going to be going back
10 in November to make sure that they've closed it out.
11 And then I believe we would update the report to say
12 that all the recommendations had been closed out.

13 Now, with the PNR review, there's been a
14 whole body of work on that. There were I think, six
15 recommendations outstanding at the time of our
16 February 2010 update. And we went through and we were
17 able to actually close out each one of those
18 recommendations. And at the time of our review, we
19 did not have any further recommendations.

20 But that's not to say we're not going to go
21 back and review the PNR program. We are going to go
22 back and do that again probably next year sometime.

1 MR. FRANCOIS: Have you all contemplated --
2 okay, so what happens if they're deficient or whether
3 they don't?

4 MS. PRESSMAN: If they're deficient or if
5 they don't?

6 MR. FRANCOIS: Yeah.

7 MS. PRESSMAN: Well, we haven't had to cross
8 that bridge yet. I really think it's in everybody's
9 best interests in these cases to implement the
10 recommendations. As I said, I think they're proactive
11 reviews. I think we can also help them identify ways
12 to implement the recommendations.

13 When I was at GAO we would give a bunch of
14 recommendations, but we weren't really there to
15 actually help them implement it. So I think the
16 benefit of us being over here is that we can help them
17 with ideas on what they need to do to close those
18 recommendations out. So I think there is an incentive
19 on all parts to move it forward to closure.

20 MR. PURCELL: Thank you. And bring us home,
21 here, Lance.

22 MR. LANCE HOFFMAN: All right, let me try to

1 bring you home. I'm struck by the semantics of what
2 you're describing. I'll tell you what I mean. The
3 title of your presentation here is "DHS Privacy
4 Compliance Reviews: Building Accountability."

5 And this reminds me of -- in my organization
6 we also have a compliance office. And I, as somebody
7 who goes and has to ask for money and get money and
8 get grants, they actually are very helpful, but I
9 cringe when I start thinking about it that way.

10 Because it's not really compliance, it's
11 more -- or put it another way, it's more than
12 compliance. It's what you're describing. It's more
13 helpful, you know another set of eyes on the problem
14 or something like that.

15 And when it describes reviews and then
16 building, it's almost two different things. Reviews
17 are looking backward and building is looking forward.

18 So my question really becomes, typically, when do you
19 get started in the life of a project? Because it
20 seems to me, the earlier you can do this within
21 reason, the better off everybody would be.

22 MS. PRESSMAN: Right. So I think earlier in

1 my comments I talked about how actually doing the
2 initial Privacy Impact Assessment really is a review.

3 Those are very intensive questions we have to go
4 through and identify, what are your policies and
5 procedures, what are you going to collect, how are you
6 going to use it, what are the privacy risks and how
7 are you going to mitigate that?

8 So I think on the front end, we're doing a
9 pretty good job of trying to identify those risks up
10 front, but what we're missing is sort of going back
11 periodically and reviewing those risks and updating
12 them. So I think that's where the review comes into
13 play.

14 So privacy baked in early is always the best
15 thing to do, but I think a review that comes before
16 you actually have to do your compliance documentation
17 refresh is also optimal.

18 MR. LANCE HOFFMAN: Does that vary in time
19 from project to project?

20 MS. PRESSMAN: I think it will -- and I also
21 don't want to give the impression that we're going to
22 do this for every single PIA that we're putting out.

1 We have a small compliance staff. Hopefully we'll get
2 more people to push this forward, but I think right
3 now we're probably going to do a risk-based approach,
4 identifying what programs and systems that we want
5 to actually do these reviews for, you know especially
6 new uses.

7 I mean social media was a really great
8 opportunity for us to put a line in the sand and say,
9 okay, we're going to approve this use of social media
10 for these purposes, but we're going to come back and
11 review it and then we're going to discuss and see if
12 this is an appropriate use of information by the
13 government.

14 MR. PURCELL: Ms. Pressman, thank you very
15 much for your comments today. It's very helpful. And
16 Mary Ellen, thank you also for your presentation
17 earlier. Members of the Committee, know no good deed
18 ever goes unpunished. We're cutting down our break
19 now in order to retrieve our schedule a bit.

20 We'll meet here again in 10 minutes, please.

21 Thank you.

22 [Whereupon, at 10:12 a.m., a brief recess

1 was taken.]

2 [Whereupon, at 10:30 a.m., the meeting
3 resumed.]

4 MR. PURCELL: Thank you, and welcome back.
5 Short reminder that we do this every time, but people
6 do need reminding. Please keep your mobile devices
7 secure and quiet during the presentation, if you
8 would, please. And if you wish to address comments to
9 the Committee later this morning, please do sign up
10 outside. There's still time to sign up at the table
11 just outside.

12 I'd like now to introduce our next speaker,
13 Mr. Steve Richards. Steve is the Associate Director
14 for Communications and Training in the DHS Privacy
15 Office, and is here to discuss training in the
16 Department. And I think that we all have a keen
17 interest in understanding more about the progress
18 they're making in terms of training.

19 Mr. Richards joined the Privacy Office in
20 November of 2009. His mission is to increase privacy
21 awareness across the Department and with the public,
22 and to strengthen the Office's communications with

1 both the public and internally.

2 Before joining the Privacy Office, Mr.
3 Richards spent 12 years at Fannie Mae in a variety of
4 different marketing functions and communications
5 functions. Mr. Richards, welcome.

6 STATEMENT OF STEVEN RICHARDS, ASSOCIATE DIRECTOR,
7 COMMUNICATIONS AND TRAINING, UNITED STATES DEPARTMENT
8 OF HOMELAND SECURITY

9 MR. RICHARDS: Thank you so much, Mr.
10 Chairman. I have a really exciting job here that I'm
11 very proud of and a very clear mission, and that is, I
12 come in every day and I help protect PII. And I think
13 it's very important when I'm training employees to get
14 them right when they come in the door and make them
15 aware of this very important issue and make the
16 message clear and also make it relevant to their job.

17 I train our new employees every two weeks.

18 We have an average class in headquarters, of 50 to 70
19 new employees at DHS and headquarters, and a lot of
20 them are very eager to get to their jobs. And they're
21 wondering, why is privacy important to them. I make
22 it very clear that it's really, really important to

1 everyone.

2 Even if you don't handle PII every day, you
3 may handle it at some point, and you also may come
4 into contact with our privacy compliance process. And
5 so it's important for you to know both our risk
6 management framework, of course, the FIPPs and to be
7 somewhat familiar with our compliance process.

8 Now, I also ask everybody a question right
9 off the bat. I ask people, how many people in the
10 room have had their privacy compromised in some
11 fashion? And I'll tell you, every class I talk to,
12 two-thirds of the hands go up, and people have had
13 everything from their wallets stolen to their home
14 broken into, they've lost their driver's license or
15 some sort of impact on their sensitive PII.

16 And it really drives the importance home of
17 this very relevant topic to everyone, and gives them
18 an empathy for the possibility that they could be
19 involved in some sort of breach here at the Department
20 and that they don't want to become a statistic in that
21 fashion.

22 So it's also important to adult learners

1 that you give them some action steps to take, and make
2 them part of the solution instead of the problem. So
3 I've developed some learning tools. One of them is in
4 your packet. This just went out last month. It's the
5 Safeguarding PII Fact Sheet. This went out to all
6 staff at DHS in August via e-mail and the intranet.

7 And I worked with Rose Bird, who heads up
8 the Privacy Incidents Department here in the Office.
9 And we came up with the top five incident types. And
10 so every time I am out training people, I train them
11 to avoid these incidents and the steps that they can
12 take to do so. So again, we get people involved right
13 from the outset so that they're prepared when they do
14 handle PII.

15 Now, TSA had an employee survey back in
16 2009, and employees in general were very happy with
17 the privacy awareness education they were receiving,
18 but they said, we need more. We need this topic to be
19 kept top of mind for us. So that's why we don't just
20 train people. We have events, we have communications,
21 we have posters.

22 I'll show you in a minute that TSA has

1 prepared Privacy Man posters, to constantly keep
2 privacy top of mind for our employees. So again, you
3 have to have training and you have to have awareness
4 as well. Next slide, please, Charlie?

5 Okay. Now that I've given you a sense of
6 how we train, I want to go over where training stands
7 right now in the Department. And we're going to start
8 with the 12 Privacy Points of Contact that I track
9 here at DHS. Eight of the 12 currently do new hire
10 training. We'd like to see that number get up to 12
11 during the next fiscal year.

12 It's very important that we train new
13 employees when they're coming in the door. But I do
14 want to note that the Culture of Privacy Awareness,
15 that's our mandatory computer-based training that is
16 required for all DHS staff, employees and contractors.

17 Eleven of the 12 components are currently
18 implementing that program.

19 It has not been implemented yet in FEMA
20 because we just got a privacy officer this year, but
21 they will be implementing that when we roll out the
22 new course in January. I'm currently working with a

1 vendor to revamp that course.

2 As I said, it's delivered via computer
3 because it's impossible to have classroom training for
4 189,000 folks effectively every year. And I want to
5 have you note that this course is only one of six
6 courses that are Congressionally mandated for all DHS
7 staff, which shows you how important the privacy topic
8 is.

9 Now, job specific training is also very
10 important. It's important to deliver training that's
11 very relevant and specific to people who handle
12 sensitive PII. And CIS and ICE are doing a great job
13 of that. They've rolled out job-specific training
14 this year to guide people through handling sensitive
15 PII specifically in their field offices. And so I'm
16 hoping to work with the other components to develop
17 training of this nature for them as well.

18 Again, my role here is to act as an advisor
19 and assistant too. Many of the Privacy Points of
20 Contact only have one person to do the entire
21 compliance function as well as training, so I am their
22 resource to help them implement best practices.

1 Let's move on to activities that have been
2 going on in the components on this slide. Fifty
3 percent of the components now have some sort of
4 activity that they're exercising to increase privacy
5 awareness.

6 US-VISIT, for instance, is going to have
7 another Privacy Week, around Halloween this year. And
8 I'm proud to say that the Secret Service just
9 announced that in November they're going to have their
10 first ever Privacy Week, so we're excited about that.

11 And again, what I do is I collect best
12 practices from these events and help leverage those
13 for the components that have not yet implemented their
14 own Privacy Week. One component this year actually
15 had a Privacy Month.

16 We also have ten of the 12 Points of
17 Contact that have developed either an intranet or an
18 extranet on DHS.gov, complete with privacy resources,
19 including compliance documentation.

20 Okay, next slide, please, Charlie?

21 Let's talk about all the wonderful work that
22 my office is doing. I've done a lot of training in my

1 career, both here and at Fannie Mae, and I've never
2 worked with so many subject matter experts that also
3 love to talk and are good at it. So it really
4 takes the burden off me.

5 We're doing a wide range of training
6 activities, and Mary Ellen already referred to a lot
7 of these. For new employees, myself and Bill
8 Holzerland on the FOIA team, cover new employees every
9 month in headquarters, and we're hitting about 150
10 staff a month, so that's not so bad.

11 I redid the new employee training. It's a
12 30-minute privacy and compliance overview. I also
13 participate every month with Civil Rights and Civil
14 Liberties here to do a one-hour Privacy and Civil
15 Rights overview for new employees.

16 I'll have you note, this is a brand new
17 course and I developed it with that office, and it's
18 now required to be taken by every employee within
19 headquarters, existing employees as well as new
20 employees, within six months of hire.

21 I already talked about the mandatory Culture
22 of Privacy awareness, which I'm revamping and hope to

1 roll out Q1 2011. And again, we have 92 percent
2 compliance on that. The other eight percent are FEMA
3 employees, and so we hope to be 100 percent compliant
4 next year.

5 Now, compliance, Renard you had asked about
6 compliance training with Jamie. Becky's team does a
7 wonderful job of training. They focus specifically on
8 the Privacy Points of Contact. They also do ad hoc
9 compliance training.

10 And every year they hold a one-day privacy
11 workshop, and that's attended by people within the
12 Department and people outside of the Department,
13 because they want to come and learn about our
14 compliance best practices, our process and our
15 documentation. So in June we had over 125 people
16 attending that one-day workshop.

17 Mary Ellen filled you in on the Fusion
18 Center staff training. We have quite a few people
19 involved in our office. I helped with Civil Rights
20 and Civil Liberties to put together the training of
21 trainers. And then Martha Landesberg, Ken Hunt, Lynn
22 Parker, have been involved in doing the actual

1 training and going out to the different centers on
2 helping on that effort.

3 And then Shannon Ballard, I'll give her
4 extra credit because she's actually in a two-day
5 presentation course right now to improve her skills as
6 a presenter. And she'll be kicking off this fall, a
7 brand new web-based course for international attaches
8 and liaisons.

9 Now, this isn't a compliance training; it's
10 a privacy policy training. She wants everybody who's
11 going internationally, when they're conducting
12 international negotiations, to be aware of how
13 important privacy policy is with that. And so she's
14 going to give them a one-hour overview of
15 international and domestic privacy policy so they'll
16 be prepared.

17 Next slide, please.

18 Now, I also mentioned the importance of
19 awareness. I remember when I interviewed a year ago
20 with Mary Ellen, I said, well, what will be my first
21 task you'd like me to accomplish, and she said, God,
22 our web site is just a mess. I need you to focus on

1 that right away.

2 And if you look at the slide now, I think it
3 looks a lot better. This is DHS.gov/privacy, and it's
4 a task-based site. So it's based on what people are
5 coming in to this site to do. And that's why we go to
6 web sites. We go to find information and perform a
7 transaction.

8 Obviously our FOIA site, as Mary Ellen
9 mentioned, gets a whole lot of requests and they keep
10 going up. So people come here primarily to submit
11 FOIA requests and get more information on that
12 process, and who they should contact within the
13 components.

14 Second, people are coming to get information
15 on Privacy Impact Assessments and SORNS and where to
16 locate those as well. So we have a nice new click-
17 through at the top with nice graphics, and we also
18 have further below a nice table of contents so people
19 can quickly come to the home page and find what
20 they're looking for pretty readily.

21 We also have a new fact sheet that I think
22 you saw at the last meeting that gives a nice two-page

1 overview of our office that I developed. We hand that
2 out at domestic and international conferences and to
3 all new employees.

4 Mary Ellen mentioned our new e-mail campaign
5 that goes out to all of our constituents. We have
6 about 300 that receive those e-mail campaigns that
7 help to position our office as a thought leader in the
8 privacy field. And you noticed that we now have a
9 banner and tag line that we use for all of our
10 external communications as well as on our Intranet.

11 Next slide, please, Charlie.

12 Now, I've also been involved in converting
13 our standalone intranet site to SharePoint, and the
14 nice thing about that conversion that took place this
15 year, is that now all the components talk to each
16 other.

17 So if somebody in FEMA wants to find out
18 about our training programs in the privacy and FOIA
19 areas, they can come to our intranet site you see here
20 and find all of our resources here. This is also a
21 nice place where contractors can come and take privacy
22 and FOIA training as well and find other resources.

1 Also posted here is the Safeguarding PII fact sheet
2 that I mentioned a little earlier.

3 Okay, last slide, please?

4 Now, I know you all were very curious at the
5 last meeting about metrics. There's no point in
6 having a training program unless you know how
7 effective it is.

8 And so currently what we're doing now is
9 we're reporting through the 803 reporting process
10 every quarter. In fact, the next report will be
11 coming up sometime this month over the next couple of
12 weeks. But I want you know that I'm going to
13 implement the Kirkpatrick Model.

14 Don Kirkpatrick developed this model back
15 when he did his thesis, University of Wisconsin, back
16 in 1959, as one of the most highly respected training
17 metrics models that's used internationally, and it has
18 four different steps here that I'll walk you through.

19 First, is learner satisfaction. Well,
20 that's kind of basic. You want to know if your
21 participants actually are getting anything out of your
22 training. And what we're going to do is implement,

1 this is really easy, folks. It's low-hanging fruit,
2 is have anonymous course evaluations.

3 The only thing that's holding us back right
4 this moment, why we haven't already implemented such
5 an easy task is because our learning management system
6 doesn't have the feature in the program. And I've
7 requested that be changed so we can implement that
8 with the rollout of the new Culture of Privacy
9 Awareness in January.

10 So it's also a good way to find out if you
11 have mistakes in your training. So we're hoping to
12 benefit from that, and obviously when you get student
13 feedback, you're able to amend your training to
14 improve it.

15 Two, we'd like to be able to measure the
16 effectiveness of our training. And the new culture
17 course will have case studies based on the most
18 prevalent privacy incidents. And they say students
19 have 90 percent better retention of what they learn if
20 they're able to implement the skills that they've
21 learned immediately.

22 So we're going to have a new course that's

1 very interactive, again, based on scenarios and
2 simulations, and we'll have people taking the new
3 rules and procedures they learn and apply them to test
4 cases.

5 Now, number three, job performance. Well it
6 would be great if we had the staff to go out and talk
7 to everybody's supervisor and say, hey, did John or
8 Jill actually implement in their job the safeguarding
9 PII skills they learned in their new employee training
10 or in their automated training?

11 Since we can't do that, the next best thing
12 we can do is to implement an annual employee survey.

13 TSA did it; ICE did it through the OIG's efforts.
14 They had a pretty good response rate, 1 to 3 percent,
15 and it helped assess whether training was actually
16 meeting its goal of helping employees perform their
17 jobs better and to reduce privacy incidents.

18 Okay, number four, and this is where the
19 rubber will hit the road. We'd like to introduce a
20 new metric. We'd like to actually match the timing of
21 any sort of training or awareness activity to privacy
22 incident reporting. So for the first example would be

1 in August.

2 As I said, I disseminated this new fact
3 sheet that has very strategic steps to reduce privacy
4 incidents. And everybody at DHS got it, so we're
5 going to be tracking each month to see if the number
6 of incidents go up, because there's also information
7 here on how to report, how to identify and report a
8 privacy incident. And we're going to be looking at
9 those statistics.

10 Also, when US-VISIT has its Privacy Week and
11 Secret Service, too, we'll be putting that into the
12 database to measure the succeeding months within those
13 components to see if reporting goes up. And if it
14 does, then we'll be looking at the incidents over
15 time, whether they -- we hope that reporting goes up
16 temporarily and then the number of incidents goes down,
17 because people have been trained on proper procedures.

18 Okay. So that's my overview of training and
19 awareness here at DHS, and I'd love to field any
20 questions from the Committee?

21 MR. PURCELL: Thank you, Mr. Richards. One
22 of the first questions I would have would be

1 clarification on the 12 Points of Contact. Tell me
2 more about the determination of the number 12, and
3 what that means? What are the 12 Points of Contact?
4 There's 22, 23 components?

5 MS. CALLAHAN: No.

6 MR. PURCELL: No?

7 MS. CALLAHAN: They combine from 22.

8 MR. PURCELL: Okay, so 12 is a universal
9 number? That is?

10 MR. RICHARDS: No, they're actually 7
11 components, but then we track different offices within
12 headquarters that have Privacy Points of Contact. So
13 I include those as another 5.

14 MR. PURCELL: All right. Okay.

15 MS. CALLAHAN: That's everybody.

16 MR. RICHARDS: Sorry for the confusion.

17 MR. PURCELL: So it's everybody. Okay,
18 fine. David, you had -- Lance.

19 MR. LANCE HOFFMAN: Okay. You mentioned a
20 couple things about wanting to be a thought leader.
21 They all come together in my mind, because it fits
22 very nicely. I like what you're saying, wanting to be

1 a thought leader.

2 I notice you have some events that have been
3 attended by people outside the Department. One thing
4 I noticed in teaching occasionally this material, I've
5 already used this thing here, the Privacy Office's
6 organization and the Culture of Privacy at DHS as an
7 example.

8 And I notice also I had, you know a couple
9 people come over from DHS to one of our seminars at
10 the University the other day, and the speaker was
11 surprised that DHS was doing so much.

12 So my question is, how much external -- I
13 understand your audience is mainly internal, I
14 believe, but how much external outreach can you do, or
15 how easy would it be for other people outside to use
16 this, if you want to be a thought leader and to pick
17 it up and use it?

18 Because it seems to me, a lot this material
19 is fairly universal and can be pretty easily adopted,
20 especially the web-based material. Oh, one more
21 question. Is there an index of all that somewhere?

22 MR. RICHARDS: Of our training efforts, you

1 mean?

2 MR. PURCELL: Yes.

3 MR. RICHARDS: Yes, we have it well
4 documented and most of it's available -- all of it's
5 available on our intranet. We don't have it on the
6 external web site because it's not relevant to people
7 outside the Department.

8 MR. PURCELL: Well, that's what I'm asking
9 you to consider because a lot of it is germane and in
10 terms of being a thought leader, it could be relevant.

11 I understand there's some stuff that's DHS specific
12 that is not. That's all I'm raising.

13 MS. CALLAHAN: So with regard to that,
14 Lance, thank you for that. We -- Steve has kind of an
15 interesting job because he's working on the internal
16 stuff but also external communication, like the e-mail
17 campaign that he's established and so on. And it's a
18 kind of a unique role for a communications officer to
19 do both. And fortunately, we were lucky because Steve
20 has both those skills.

21 In terms of the external communication, it's
22 certainly something that as you know is important to

1 me for transparency reasons, but in terms of the
2 training, I agree with Steve that I'm not sure that
3 specific training is germane for an external audience.

4 That's very specific, but it's certainly germane to
5 leverage the assets for all of the different
6 components.

7 With that said, we're trying -- the guide I
8 think is a better example of what would be a holistic
9 view of the DHS office at large. I think that the
10 training may be too kind of granular, or inside
11 baseball, so to speak. But if people have an interest
12 in it, we're of course willing to share it. It just
13 seems to me to be focused more on the internal
14 audience than the external.

15 MR. PURCELL: Perhaps at some point Steve
16 will take the Committee through some of that training
17 and in some detail.

18 MR. LANCE HOFFMAN: That would be nice.

19 MR. PURCELL: Something we're not going to
20 do today, but I think the Committee has an interest in
21 taking a look and getting some instructions as to how
22 you're doing that. It'd be very interesting. Ramon.

1 MR. BARQUIN: I just want to go back again
2 to this issue, because I think it's extremely
3 important. This is the external, and it's not just
4 communication, but I think there's the element of
5 training. And I wanted to focus on the area of
6 redress.

7 I mean, there is such need for understanding
8 and training on the how-to of redress and the
9 different aspects of this, that I just wanted to at
10 least put in my two cents in favor of consideration.
11 Because you've got a lot of the elements in place.

12 MS. CALLAHAN: That's a great idea, Ramon.
13 That's a little bit different, that's kind of training
14 the public, but at the same time I think that's a good
15 idea. What Steve's talking about is training the
16 189,000 DHS employees.

17 But I appreciate your point, and I think
18 that we can work on trying to -- we've done some
19 public stuff, but not in kind of a consumable way.
20 And that's a great idea.

21 MR. BARQUIN: Okay, question that okay, if
22 it is not within the purview of this part of your

1 training program, where does it fall in DHS? Because
2 there is a huge need for public training, because a
3 lot of the problems the Department often faces is a
4 result of lack of understanding of what is going on.

5 MS. CALLAHAN: So I would actually call it
6 public awareness rather than training, because I don't
7 think it's my job to train the public. But there are
8 other elements in the Department that work on redress
9 issues. But I think an awareness campaign is one that
10 I certainly can take back, and I appreciate the
11 recommendation.

12 MR. PURCELL: Yeah, a communications
13 director might have a problem with a CPO training the
14 American public from a DHS perspective. David,
15 please.

16 MR. DAVID HOFFMAN: Steve, I first would
17 like to commend you. I think this program is
18 absolutely fantastic, and a whole step change above
19 where the program has been, which was good to begin
20 with. But this is absolutely fantastic.

21 As you move forward, I'm wondering
22 strategically, what I've noticed among many private

1 enterprises with large numbers of employees,
2 especially with diverse business lines, once they've
3 solidified around a general employee awareness and
4 education program, many of them have then looked to
5 integrate the program into existing business processes
6 within the business so that people are getting
7 training and awareness materials at the point in time
8 where they're actually executing on a business
9 function, which also allows you to be able to measure
10 it more effectively because it can be measured at the
11 same time.

12 So for example, a privacy by design process
13 might have been implemented with a Privacy Impact
14 Assessment or the threshold analysis material that
15 would pop up automatically for individuals, and you
16 could be able to understand and measure how many times
17 that's done.

18 Another example might be working with HR to
19 say, let's integrate privacy as a component of every
20 employee's annual performance review, so that every
21 employee should at least be asked, how did
22 the employee do this year on integrating privacy?

1 I just wanted to understand the degree of
2 which you've thought about whether that would be an
3 evolution that you guys would want to move to in the
4 next release of where you want to go?

5 MR. RICHARDS: Well, I think that's one
6 thing we're looking at in moving or pushing out the
7 job-specific training that ICE and CIS have already
8 started. Because again, they're hitting people when
9 they're implementing the training programs around
10 safeguarding PII. So it's very relevant and the
11 timing is good there.

12 And also, Becky Richards is leading an
13 effort on our intranet, so that when people are
14 posting PII, they're going to be given information to
15 make sure that they don't post sensitive PII where
16 they're not supposed to be. So there'll be new bells
17 and whistles within, built into our intranet to make
18 sure that sensitive PII does not get posted in a
19 manner which is not permissible. So that's one new
20 process that's going to start kicking off Department-
21 wide in December through next year. So that'll be a
22 good safeguard there.

1 And again, we're also working with the
2 COTRs around the agency to try to make sure that
3 contractors that are on boarded are receiving
4 training, okay, and that they're getting it actually
5 before they start, so that they're prepared when they
6 start handling any sort of PII.

7 MR. DAVID HOFFMAN: So I think that's all
8 very good. I would say I would encourage you to
9 continue to look for places in the process where
10 deeper substantive information can get to people at
11 the points where they're actually doing their job so
12 that they can self-educate themselves and have those
13 materials available. That's where I think people who
14 have -- my peers in different corporations have gotten
15 some of the most value of what they've done.

16 MR. RICHARDS: That's a great suggestion,
17 and also, it goes back to the relevancy issue as well.

18 MR. DAVID HOFFMAN: Right.

19 MR. RICHARDS: Oh, and I also wanted to
20 reinforce a point around the compliance team's one-day
21 workshop they have every year, that the public is
22 invited to that. And Lance, you were talking about

1 our thought leadership. I think in particular it
2 applies to our privacy compliance documentation.

3 And we often get calls from other government
4 agencies who basically want to copy all of our
5 documents and just change the name of the agency. And
6 we tell them, why don't you come over and talk to us,
7 and we'll help you sort of transition these documents
8 so that they're more customized to meet your needs.
9 But we're very flattered -

10 MS. CALLAHAN: But we let them take the
11 documents. There's no IP rights to those documents.
12 For example, the Government Printing Office is
13 printing several of our documents for government-wide
14 distribution.

15 MR. PURCELL: Excellent. So Mr. Pattinson.

16 MR. PATTINSON: Thank you. Steve, I'm
17 involved much like you in some elements of training
18 and compliance for my organization. And a couple of
19 things that we've learned, and sending these kind of
20 things out is terrific, but you also have to get the
21 individual to read it and to acknowledge that they
22 read it.

1 So we've worked in the principle that
2 pushing the information out is good, but you also need
3 to acknowledge that they have digested it and signed
4 something or sent an e-mail back or whatever. We then
5 kind of moved on from the kind of pushing things out
6 as well as the training, and I see you have a
7 gargantuan task of training all these people every
8 month.

9 What we've, you know a suggestion today up
10 at the table here, is online training. Once you've
11 done the official induction training and so on, is
12 that on an annual or biannual basis, two years,
13 whatever, you do a short 15-minute interactive online
14 training.

15 They're very simple to set up, and you can
16 ask them a series of questions or train them and go
17 through a series of refresher questions, and kind of
18 score them. And if they get over a certain percent,
19 they've got that kind of badge to continue as trained
20 and knowledgeable.

21 You know otherwise, a one time as a new
22 hire, and without that kind of refresher, after a year

1 or two years, some of the policies change or some of
2 the techniques change, and it's a question of keeping
3 them fresh.

4 So looking at what you're doing, which is
5 fabulous, I'm kind of looking down the road as to how
6 you could continue that awareness and get some
7 positive acknowledgment that the employees are
8 actively involved and still understanding the
9 principles and the practices by having some sort of
10 online or simple refresher, where you're getting
11 feedback, that yes, all these employees have done it,
12 or wait a minute, we've got a whole bunch of people
13 here that haven't done it, why not, and what could we
14 do to make sure that they are still aware and up to
15 speed with the latest recommendations and policies?

16 MR. RICHARDS: Well, actually, Neville, that
17 is covered, and maybe I didn't make it clear, but the
18 Culture of Privacy Awareness that I'm redoing for
19 January, that is an annual requirement. That's a
20 Congressional requirement, and that is a 20, it's
21 going to be probably 20-minute training.

22 But that's the 92 percent threshold that

1 we're meeting now, that 92 percent of our 189,000
2 employees are taking that every year. In having tests
3 and quizzes, that can be a little tricky with the
4 unions, frankly. So we get around that by having the
5 scenarios that I'm going to be implementing.

6 We're going to have a coach. It's going to
7 be an animation module, and we're going to have a
8 coach guide you through the compliance process and
9 also safeguarding sensitive PII. And then have you go
10 through some models where you have to make some
11 decisions.

12 And so people will sort of be scored on
13 that, how they get through those case scenarios. But
14 then, again, it's not just for new employees, so I did
15 make the requirement clear that it is required within
16 six weeks of hire, but then it's annually thereafter.

17 MR. PATTINSON: Terrific.

18 MR. RICHARDS: And I'll make sure that the
19 course isn't just static, that we'll keep it updated
20 every year to comply with the most prevalent incident
21 types.

22 MR. PATTINSON: Great, thank you.

1 MR. PURCELL: And Kirk, please.

2 MR. HERATH: I think you just answered my
3 question. So it's -- they have to take the training
4 within six weeks of hire?

5 MR. RICHARDS: Right.

6 MR. HERATH: But you got 92 percent that
7 have taken it. What's the ramifications for not
8 taking it?

9 MR. RICHARDS: You get -- it's delivered
10 through each learning management system and every
11 component, and so an employee would get reminders
12 before, and then if you're overdue and as well, if
13 you're overdue, then a notice goes to your supervisor,
14 and it's up to the supervisor then to inform the
15 employee that they're overdue and they'll be penalized
16 on their review if they don't take the course.

17 MR. HERATH: So there's no -- there's not
18 any termination if they don't take it, for
19 insubordination or anything like that?

20 MR. RICHARDS: Not that I'm aware of. But
21 again, the rules are component-based, so it's up to
22 each component to enforce that rule.

1 Oh, and I did want to add that we're adding
2 -- with the new course, we're adding an acknowledgment
3 at the end, and so that'll show -- and there is legal
4 language in there in that employee acknowledgment,
5 that they're aware of their responsibilities to
6 protect PII and also of the consequences of failure to
7 protect PII. So that's new that'll be added with the
8 new course in January.

9 MR. HERATH: One last thing. The contractor
10 training was a gap that we found a couple years ago,
11 and one way that we enforce it is if that contractor
12 doesn't take the training within two weeks of hire,
13 they don't get paid.

14 MR. RICHARDS: That's a pretty strong
15 enforcement.

16 MR. HERATH: We have basically 100 percent.
17 Thank you.

18 MR. PURCELL: Mr. Richards, I think the
19 Committee welcomes the comments that you've made, and
20 all of the progress that you've demonstrated that
21 you've made so far in this awareness and training
22 program. So thank you very, very much for your

1 comments. We appreciate it.

2 MR. RICHARDS: Thank you.

3 MR. PURCELL: Our next speaker is Lawrence
4 Castelli. Mr. Castelli is the Privacy Officer for
5 Customs and Border Protection Component of DHS and is
6 responsible for monitoring that component's compliance
7 with all the federal privacy laws and regulations,
8 implementing corrective, remedial or preventative
9 actions, and notifying the DHS Privacy Office of
10 issues of non-compliance when that is necessary.

11 He is authorized to act upon all privacy
12 matters within CBP and to require all offices within
13 CBP to coordinate policy issuances that touch upon
14 privacy with the CBP Privacy Officer.

15 Prior to assuming that current position, Mr.
16 Castelli served as the Chief of CBP's Privacy Act
17 Policy and Procedures Branch within the Office of
18 International Trade, and he did begin his legal career
19 in the Customs Service in 1989 and has practiced in
20 the Freedom of Information Act and privacy areas since
21 1996.

22 Mr. Castelli, welcome.

1 MR. CASTELLI: Thank you, Mr. Chairman.

2 Thank you, Committee for having me here and Mary
3 Ellen. You know, when I think I last spoke with you
4 when we were in Vegas.

5 MS. CALLAHAN: There's a lot of border work
6 in Vegas.

7 MR. CASTELLI: Well, you know, I believe
8 they have an international airport and we like to
9 think of that as the functional equivalent of the
10 border.

11 STATEMENT OF LAWRENCE CASTELLI, PRIVACY OFFICER,
12 CUSTOMS AND BORDER PROTECTION, UNITED STATES
13 DEPARTMENT OF HOMELAND SECURITY

14 MR. CASTELLI: Fortunately, in that instance
15 not everything that happened stayed in Vegas. But
16 that was in 2008, and so what I thought I would do,
17 just as sort of a brief introduction is sort of catch
18 us up from what we've been doing since then.

19 CBP, Customs and Border Protection, is a
20 border agency. And I think it's safest to say that
21 the theme that I've chosen to cover my remarks, but
22 also to address generally in how my staff approaches

1 privacy within CBP is to look at how we would
2 operationalize privacy, how we would implement and
3 embed privacy compliance into the culture of CBP.

4 And it's something that has been there for a
5 long time. I think it's just something that needed to
6 be spread out uniformly throughout the entire Customs
7 and Border Protection. It's something that we need to
8 constantly emphasize.

9 One of the first things we did following in
10 December of 2008 is as part of the last
11 Administration's effort, to transition legacy System
12 of Records Notices to DHS, we started on the process
13 of basically revisiting some of our old System of
14 Records Notices to try to decide what should be broken
15 up.

16 This question of transparency that often
17 comes up was one of the issues we wanted to tackle at
18 that time. Following that, we then began to look at
19 some other staffing issues in terms of how better to
20 implement privacy.

21 One of those changes was last August, or
22 actually last September, when I was made the CBP

1 Privacy Officer, and my reporting structure changed
2 from being within an office to basically reporting
3 through an assistant commissioner to the Commissioner.

4 This higher visibility allowed me then to
5 get out and contact other assistant commissioners in
6 other functional areas to work with them on how they
7 were allowing privacy to be part of their calculus
8 when they were beginning new programs.

9 Most notably, we do this with the Office of
10 Information Technology. We meet monthly to discuss
11 how new IT development is being done and how privacy
12 compliance is working there, both with the Privacy
13 Threshold Analyses and then from there on into the
14 Privacy Impact Assessments and System of Records
15 Notices.

16 In addition, we look at other privacy
17 implementation, just in terms of border practices. We
18 also look at it in terms of trade practices. Privacy
19 is something that we have always, CBP has always taken
20 a look at privacy as being something that crosses its
21 two principal missions.

22 The principal missions of CBP are border

1 security and trade facilitation. Increasingly, what
2 we find in trade facilitation is an emphasis on
3 obtaining data and obtaining data early, in advance of
4 when the merchandise arrives.

5 And what we find when we look at that data
6 is it's not always about what's in the box that
7 matters as much as who packed the box, who carried the
8 box, who's transporting the box, who shipped it and
9 who bought it. Because those parties are often the
10 people who are going to use that.

11 And in the same way that when we look at
12 what the Privacy Act and our own internal guidance
13 tells us in terms of like the Fair Information
14 Practice Principles, one of the critical points there
15 is often this concept of use. How are you going to
16 use information?

17 Well, one of the things we look at in a
18 trading context is whose information is it, how is it
19 being used. And we look at it not only in that
20 regard, partly from a border security and a compliance
21 process, but we also look at it in terms of our
22 mission to share that information.

1 Let me just say that CBP is roughly 58,000
2 employees. The vast majority of these employees are
3 on the front line, serving in the Office of the Border
4 Patrol or serving in the Office of Field Operations at
5 our ports of entry, as we sort of transform the
6 privacy practice at CBP and trying to achieve a
7 greater transparency where it's appropriate.

8 Obviously, a fair amount of the information
9 we collect in different contexts, we need to keep
10 confidential, confidential because it pertains to an
11 individual and it's personal, confidential because it
12 pertains to a business and it's a trade secret.

13 But even in those contexts, it would be
14 wrong to say that when we say we want to keep it
15 confidential, we want to keep it confidential from
16 everyone. In the same way that a person needs to be
17 able to know what information the government has
18 collected about them, this is the access concept that
19 is embedded in the Privacy Act.

20 And this is something that as we transform
21 the System of Records Notices for CBP, we looked at
22 very closely at ways that we could affect that

1 practice but not interfere with what would be our law
2 enforcement mission as well. And what I mean by that
3 is typically when we collect information from you as a
4 member of the public, we ask you to submit something.

5 And the way I like to describe this to
6 people is, when I ask you to give me something, I ask
7 you to fill out a form, I ask you to put something
8 down on a piece of paper, you could have made a
9 photocopy of that before you handed it to me.

10 Not that we have photocopiers ready for you
11 to do that, but assuming we did, you could have. And
12 then you'd have a copy of what you handed into the
13 government. Well, I think as a concept there's no
14 reason why you can't get that photocopy after you've
15 handed that information to the government.

16 I mean I think one of the principal concepts
17 behind the access rights in the Privacy Act is to
18 enable you to get that information back. What did I
19 give you? It informs you when you're seeking to make
20 amendment, it informs you in a number of different
21 ways.

22 Now, that's not to say that if when you

1 handed it to us we've done something with it, we've
2 worked it up, we've added information, that you would
3 necessarily get that information. But I think as a
4 basic concept, you need to be able to get back what
5 you gave us.

6 This is certainly a practice we've always
7 followed in the trade realm, where we've always
8 provided traders with copies of their entry
9 information. We won't provide it to anyone else. I
10 mean when you tell us how much you paid and where you
11 bought the merchandise you're importing, we won't give
12 that to someone else unless you authorize it, but we
13 will give it back to you.

14 And I think in the same way, if you're a
15 member of the traveling public or if you're just
16 crossing the border because you live in a border
17 community, you should be able to get that information
18 back.

19 And if you have -- you know for instance, if
20 you have a Trusted Traveler card because you
21 frequently cross, you should be able to know what, see
22 that information and check it on a regular basis.

1 One of the ways that we've actually looked
2 at embedding privacy, and I think as an example, a
3 good example that I would choose would be to look at
4 the Privacy Impact Assessment that we released last
5 year on the border search of electronic devices.

6 This was an issue that arose in the press
7 and was something that we needed to address. We
8 needed to discuss this. We needed to get out and have
9 the public be aware of what these practices were. And
10 as we were proceeding with developing this Privacy
11 Impact Assessment, we also looked at some of the
12 guidance that existed to the field officers.

13 And this whole process of having privacy and
14 having our counsel's office and having the program
15 officers involved in revisiting and reviewing what
16 these practices were, and in having a very healthy
17 discussion about, how can we best do this, how can we
18 do this in a way that doesn't compromise the law
19 enforcement mission, but still is sensitive to the
20 fact that the vast majority of the traveling public is
21 just that they're traveling public; they're not
22 offending anyone, they're not doing anything wrong,

1 they're not violating a law.

2 Yes, it's true some do, but that's -- but
3 the vast majority don't. And so we need to, in that
4 same way that we facilitate trade, we need to focus
5 on, there is a mission to facilitate travel.

6 One of the other things that we were looking
7 at doing as part of this transformation, as I
8 mentioned earlier when we revised System of Records
9 Notices, we looked at the Treasury Enforcement
10 Communications System, which is the old -- the acronym
11 is TECS.

12 And that was the old system for a long time.

13 That was our border screening system. In December of
14 2008, we effectively broke up TECS into five different
15 System of Records Notices.

16 It's not that we really changed the
17 functionality so much of the system in terms of the
18 information that was collected, but we wanted to get
19 out there and let people know, these are the different
20 types of information that we collect from you at the
21 border, and how we collect it.

22 And there may be differing rights. And so

1 we took TECS and we kept the acronym because we felt
2 that the public was already aware of it, and they
3 needed to be comfortable that that wasn't changing.

4 We had previously taken the Advance
5 Passenger Information System, APIS, out of TECS. We
6 also took the Nonimmigrant Inspection System, which is
7 where the I-94 information is being maintained, we
8 took that out of TECS.

9 We had previously noted that the Border
10 Crossing Information System, that basic system when
11 you cross the border and we collect some biographic
12 data, as well as a date and time stamp about your
13 crossing activity.

14 And then lastly, there was the SEACATS, the
15 Seized Assets and Case Tracking System, which is when
16 there was a penalty that was developed based on your
17 interaction or we made a seizure, that's where that
18 case information would go.

19 And one of the reasons we wanted to do this,
20 to break out these systems, was I think a legitimate
21 criticism of CBP and the Custom Service and the
22 Immigration and Naturalization Service before it, was

1 that we had a tendency to -- well, frankly, TECS was
2 just -- the old joke about TECS was it was in there.
3 Where's this? Oh, it's in TECS. Everything was in
4 TECS.

5 And we got very comfortable with, let's just
6 amend TECS and add another category of data, add
7 another class of individual about whom we'll collect
8 information. And I think that that's important that
9 at some level you're trying to notice it, but
10 realistically if the public's going to read this
11 notice, if they're the ones who are to benefit from
12 that notice, if you keep throwing it all into the same
13 system, they get lost. They're not going to recognize
14 that.

15 And so I think that was one of the reasons
16 why we wanted to break that out. I mean, as another
17 example, one of the other systems we started to break
18 out or to basically just consolidate legacy systems
19 from was the Global Enrollment System, which is our --
20 that's the System of Records Notice we have out there,
21 essentially for Trusted Traveler or Registered
22 Traveler programs.

1 If you have a Global Entry card, if you have
2 a NEXUS or a FAST or SENTRI, those are the principals.

3 But even some of the local boater options -- and I
4 don't know if you do any pleasure boating in the
5 coastal areas, but if you do, those systems are
6 covered by the Global Enrollment System as well.

7 I mean the intent of Global Enrollment was
8 basically to say, if you want to -- if we're going to
9 have some limited biographic information about you, as
10 a way of expediting your rearrival to the United
11 States, this is where we will maintain it. And we
12 will give you a credential to facilitate that.

13 In addition, as I said earlier, CBP because
14 of our long involvement with trade, we also have a
15 number of programs where we do screening of persons
16 involved in trade. And I purposely made sure I wrote
17 it out, because I knew you would really like the name
18 of this SORN. We call it, the Persons Engaged in
19 International Trade in Customs and Border Protection
20 Licensed/Regulated Activities. It's a bit of a
21 mouthful.

22 Someone asked me, well, what's in that one?

1 And I said, this is -- we used to have a SORN for
2 Cartmen and we used to have one for Lightermen.
3 Cartmen are truckers; Lightermen are the small boats,
4 commercial boats.

5 And then we would regulate brokers, and
6 other persons who were freight forwarders and the
7 like, who were given access, who were given
8 essentially passes or credentials that allowed them
9 access to custom-controlled space at the various port
10 facilities, because they had to conduct business.

11 And so originally the thought was, well,
12 we'll throw them all into the Global Enrollment
13 System. And our thought at that point when we were
14 talking with the operational and the IT staff was to
15 say, no, we strongly recommend against that.

16 And we recommend against it because you need
17 to think of your Trusted Travelers as a more public
18 facing. These are persons who are basically
19 traveling. They're engaged in a border-crossing
20 activity, but they're engaged in it basically as part
21 of either facilitating their business in terms of
22 travel, or for pleasure.

1 Whereas, the other group of individuals
2 we're looking at, you're giving access to a facility
3 generally, into a customs-controlled space. And so
4 the type of background check you're doing on them is a
5 little bit more involved, and the security concerns
6 and their frequency with which they may be actually
7 entering that space is greater. And so you have a
8 different approach, you have a different concept.

9 And so that was how we wanted to -- those
10 are I think a couple examples of how we were looking
11 at transforming our compliance practice. The other
12 area where -- and I have -- as part of my staff, what
13 I've tried to do is create two different practice
14 groups.

15 I have one that handles mostly privacy
16 compliance and I have another that handles information
17 sharing. And information sharing of course, is an
18 area where increasingly CBP is moving -- is being
19 pushed to the forefront to be involved.

20 Our role at the border puts us in a position
21 where we collect a lot of information. And when we
22 were in Vegas two years ago, we were talking about the

1 Fusion Center that was there. We toured that Fusion
2 Center, and there was a lot of discussion about how to
3 use fusion centers. And that discussion has
4 continued. And one of the issues that continually
5 comes up there is how do we supply information? How
6 is that information safeguarded, and how is it used
7 effectively?

8 And used effectively can be two different
9 ways. They're used effectively in the sense of, how
10 is collective action coming out of a task force or a
11 Fusion Center going to happen, and used effectively is
12 also, how do individual members of a task force or a
13 fusion center, how did they migrate data out of that
14 so that they can take individual action? Because this
15 is one of the other concerns increasingly that we're
16 looking at.

17 We're seeing this particularly in the trade
18 arena, where there's been more emphasis placed on
19 import safety and food safety missions. As part of
20 that, not only are we looking to develop -- well, CBP
21 has already developed a Commercial Targeting and
22 Analysis Center within its Office of International

1 Trade. This is a recognition that the targeting
2 centers that we have, the National Targeting Center
3 for Cargo, frankly is very focused on border security
4 issues, as it should be.

5 And it's not so much that it couldn't also
6 focus on import safety and food safety concerns; it's
7 just that at the end of the day, I think what you find
8 is each of us can only spend so much time on any one
9 task. And the more people you put in one room, it's
10 not always the most effective way for that, for a
11 task to be accomplished in that room.

12 By segregating your targeting staffs and
13 letting them focus on more specific concepts, I think
14 you also create a way to bring more people to the
15 table, because the people who are focused on the
16 security side of it are not necessarily always looking
17 for the lead paint toys. Whereas the people on the
18 import safety side can be more focused on that, and
19 you can bring in other agencies to work with you in
20 that regard.

21 Again, though, the challenge becomes, how do
22 we ensure that those FIPPs principles that we've become

1 so good at putting into our System of Records Notices,
2 that we've become so good at ensuring we discuss in
3 Privacy Impact Assessments, how do we see those
4 translated into our Memorandum of Understanding, into
5 the various Information Sharing Access Agreements that
6 we create to support these centers or these Fusion
7 Centers, these task forces where we're going to
8 coordinate with state and with local, with other
9 federal, and in some cases even with foreign entities.

10 This is one of the challenges that we're
11 continuing to work on. DHS has an Information Sharing
12 Coordinating Council. The CBP representative to that
13 is in the Office of Intelligence and Operational
14 Coordination, and one of my staff works closely with
15 that individual to attend those meetings and to
16 provide assistance and guidance on these concerns.

17 What we have done and what we continue to do
18 is make sure that in any of these agreements that we
19 draft we have confidentiality sections that address
20 the questions of specificity regarding use; the
21 limitations on how long the data will be retained;
22 minimization concepts with respect to how much data do

1 you need.

2 I mean the typical request for information
3 sharing starts out as, well, just give me everything
4 and then I'll figure out if I need to look at it. And
5 our typical response is, we need a little bit more
6 information.

7 One of the most effective things I try to
8 imbue in my staff is, the answer isn't supposed to be
9 no. The answer isn't supposed to be yes. Until you
10 have enough information to properly evaluate a
11 request, particularly in an information sharing
12 context, the answer needs to be more along the lines
13 of, maybe or can you help me understand it better?

14 Because too often, even when something
15 starts out as a very broad request and your gut
16 reaction is to simply say no, that can't ever happen,
17 what you find is you sort of, I don't know, peel back
18 the onion so to speak, is that there actually is a
19 legitimate purpose in there that you need to call out
20 and identify and you need to recognize.

21 And in an operational context, too often
22 it's sort of, I need it, I need it now and I need it

1 because I have to do something with it immediately.
2 And in the same way that when you have -- when an
3 officer for instance, writes up a report, they have to
4 be able to articulate something about what it is they
5 saw and why they took the action they did.

6 That's principally what we look to do. We
7 look to do that ingrained in the MOUs and we look to
8 do that in what I would point to as our -- we call
9 them Letters of Authorization.

10 Basically a Letter of Authorization or an
11 exchange is when your MOU doesn't cover all the
12 instances of the request that might be coming in, you
13 need to have a stopgap. You need to have something
14 there that allows for that un-contemplated exchange at
15 the time of the drafting of the MOU.

16 And that's how we usually do it is with a
17 letter, and we look at those letters as a way of going
18 forward, how do we keep MOUs to be living documents?
19 Well, one is you look at where have been the bulk of
20 exchanges that didn't fall within the rubric of the
21 MOU, and do we need to expand the MOU to address that
22 in the future?

1 An area where we're looking at enhanced
2 information sharing is with regard to the automated
3 commercial environment in the International Trade Data
4 System, the ITDs, is the -- it's an interface/portal
5 for government agencies to share entry information,
6 import information and manifest information, and
7 potentially in the future, even export information, as
8 merchandise is arriving or leaving.

9 And again, I emphasize to you -- and a lot
10 of this trade data, it is about the commodities, it is
11 about the widgets, it's about the price, it's about
12 where was it purchased and where is it going. But
13 it's also about the individuals involved. And
14 oftentimes, we need to be very cautious about how that
15 information is being used, because it does have
16 sensitive information about the individuals.

17 Certainly large corporations, you don't have
18 as much individual identification, but in small
19 businesses, a lot of the small businesses are --
20 frankly, what you see is people using a tax
21 identification number as their importer of record
22 number.

1 For many of us, our tax identification
2 number in a personal context is our social security
3 number. This is a number that you're putting on a
4 document that you're sharing with people, that you're
5 giving to the government. And one of the reasons why
6 we stress why people need to be very careful in how
7 they handle this information is because of the
8 sensitivity of that type of a number being on those
9 documents.

10 Lastly, one of the last things I think I
11 want to talk about is training. I know we just
12 listened to Steve give a great presentation on
13 Departmentally what training is out there, and
14 certainly we try to work with Steve on our training.
15 And what we're trying to do actually with Steve is do
16 more with our online training, more with getting
17 training into CBP's Virtual Learning Center, which is
18 an internal IT space where we do a lot of online
19 training.

20 With regard to Mr. Herath's question about,
21 what do you do with compliance for not training, what
22 I would say is, CBP for the longest time has had two

1 principal training courses that you're required to
2 take before you can access administrative systems.
3 One is the General Privacy Awareness course and the
4 other is the TECS Privacy Awareness course. In order
5 to get into the administrative systems, the general
6 administrative systems, you have to take the general
7 course.

8 And this is the systems about your leave,
9 about travel, about access to other training sites and
10 the like. Generally, this information, this is
11 privacy and security awareness about how you can and
12 cannot share information as it relates typically to
13 yourself.

14 The TECS Privacy Awareness course, which is
15 mandatory for anyone who will have access to TECS.
16 And actually we did get through the unions with this,
17 you actually have to pass the test at the end. It's
18 30 questions, and basically passing is, you're only
19 allowed three wrong answers.

20 So you need a 90 percent or better in order
21 to pass this test. You can take it as many times as
22 you want, but obviously if you don't pass the test you

1 can't have access to TECS.

2 And for most of our officers on the front
3 line, if you can't have access to TECS, then frankly
4 you can't have access to the IT systems you need to do
5 your work, because the TECS Privacy Awareness course
6 is our foundation for if you want to have access to
7 the Automated Targeting System, and for any of the
8 other IT systems that we use to support the
9 enforcement mission.

10 So I'm not going to say that you lose your
11 job because you can't pass the test, but at a certain
12 point if you're having trouble doing that it becomes a
13 problem. And so that's one way we do it.

14 We've also -- one of the things we're
15 looking at now with this Virtual Learning Center is
16 trying to get out there to the employee audience, to
17 the CBP audience, with more training on the awareness
18 issues. I would note, both the General Privacy
19 Awareness course and the TECS Privacy Awareness course
20 are required to be taken and retaken annually as a way
21 of reinforcing these concepts.

22 The other thing we try to do is we have

1 rolled out training to points of contact at the
2 various ports, and this is more focused on the
3 information sharing side. It's to make those persons
4 who are directly responsible for handling information
5 sharing requests more aware of the types of concepts
6 they need to be considering when they're processing
7 these requests. And that is typically more a
8 classroom setting.

9 I guess in conclusion, I've touched on I
10 think some of the high points of what it is we do. No
11 disrespect to Rose, we also handle the -- Rose Bird,
12 that is -- we also handle the privacy incidents for
13 all of CBP and we spend a lot of time working with
14 Rose and her staff, as well as the Security Operations
15 Center, negotiating the remediation of those
16 incidents.

17 But insofar as the focus of this Committee
18 seems to be more -- or at least with CBP -- seems to
19 be more on the public, I've tried to emphasize more I
20 think our activities with the public. I'm sure you
21 have questions?

22 MR. PURCELL: Oh, we always have questions.

1 Thank you, Mr. Castelli. I'm going to turn directly
2 to our members here. David.

3 MR. DAVID HOFFMAN: Mr. Castelli, thank you
4 very much for coming. Your field agents have a very
5 difficult and critically important function. We got
6 to see a lot of that firsthand at several of our
7 visits out, particularly in Detroit, I think, is a
8 place where we got to see that.

9 While we were in Detroit, we also got to
10 hear from a number of groups who expressed concern
11 about some of the information that was collected at
12 the border, in more of an ad hoc manner by field
13 agents who were doing their jobs.

14 And at that point in time, when we had asked
15 during a meeting like this, what were the policies in
16 place for CBP, about what questions they will ask and
17 what questions will they not ask, and these were
18 particularly concerns about questions around religious
19 practices and how people were exercising their First
20 Amendment rights.

21 We were told by a person from CBP that there
22 were no policies about what could be asked and what

1 could not be asked at the border, because that would
2 be restraining the ability of the field agents to
3 effectively do their job and they needed to have full
4 freedom to do that.

5 I suspect that that -- I have been told
6 subsequently that that's not fully accurate, and that
7 there's quite a bit of training done on how to be
8 respectful. I wonder -- and this is then related to
9 the collection and confiscation of electronic devices.

10 We also I think heard last year, a lot of data about
11 -- actually the confiscation of electronic devices was
12 actually fairly rare.

13 I'm wondering if there's information that's
14 getting out to the public to provide some transparency
15 about the efforts that you're taking so that there
16 aren't questions that are asked that people would deem
17 to be generally -- they generally might deem to be
18 offensive, or data that's getting out about the
19 digital devices and that it's actually very rare. It
20 concerns me that I don't think that message is getting
21 out.

22 MR. CASTELLI: Well, I think we do -- it's

1 my understanding that we do make available through the
2 web site information about our general sort of
3 aggregate searches.

4 MR. DAVID HOFFMAN: It's in the report?

5 MR. CASTELLI: Yes. And as Mary Ellen has
6 so graciously pointed out, in the report we also do
7 talk about this. I mean, we do periodically update
8 Capitol Hill with regard to the types of searches that
9 are being conducted.

10 The report I know did an exhaustive analysis
11 of the training that's out there. Your other, your
12 comment about what the previous response was is we
13 don't want to restrict what our officers do at the
14 border. You're correct in saying that that probably
15 should have been a more nuanced response.

16 The reality is, there is a lot of training
17 on a variety of sensitivities, but certainly in terms
18 of -- dating back to 1998 when we first had an
19 independent commission do a report on racial profiling
20 with respect to how we were doing border screening.
21 And there was guidance and training that came out of
22 that, and that's been part of the basic and advanced

1 training courses for all officers who work at the
2 border.

3 And that can amount anywhere from 16 to 25
4 hours worth of training in a classroom setting, where
5 you're doing a lot of different -- where you're doing
6 role playing as well as talking generally about what
7 the concepts are, about the fact that the point is to
8 focus on objective criteria and objective facts, not
9 on what necessarily the person you're seeing so much.

10 And by that what I mean is, not on their
11 appearance, not on whatever you might choose to
12 project to them, but more on other indicia. Are they
13 nervous, or wearing a heavy jacket and it's July
14 and it's 120 degrees, that kind of an issue.

15 I think we can -- I'm trying to think in
16 terms of where we were --

17 MR. DAVID HOFFMAN: Maybe I could just
18 follow up real quickly --

19 MR. CASTELLI: Yeah.

20 MR. DAVID HOFFMAN: -- to provide a little
21 bit more direction to that comment. I wonder if there
22 would be a lot of value in creating a policy and then

1 holding that policy out publicly, that embraces the
2 data minimization fit for the job that the field
3 agents would do, and provide some real definition,
4 particularly around sensitive data categories and when
5 it would be appropriate and when it would be
6 inappropriate to ask that.

7 Based on what we -- the Committee at least
8 heard from representatives of the Arab-American
9 community in Detroit. I at least came away with that
10 that would go a long way in addressing many of their
11 concerns.

12 And then your answer wouldn't have to be
13 real nuanced, and I actually appreciate, given the
14 function that the field agents have, the need for the
15 nuance, but I think there's something that's missing
16 there to communicate out how the Department does feel
17 that that data needs to be protected and minimized.

18 Think so?

19 MR. CASTELLI: I think what we have done
20 currently in, if you look at like for instance, the
21 Border Search PIA, the efforts we put into discussing
22 when it's appropriate to collect certain information,

1 the steps you go through, how the sort of what I would
2 call -- I don't want to say checks and balances, but
3 the procedural process, the fact that the PIA includes
4 the CBP directive, which is our policy.

5 That is, that was a policy that went out to
6 all officers. It basically establishes for them their
7 direct guidance as to, here's your practice, here are
8 the procedures you will follow.

9 The same guidance that we gave them
10 internally through musters, we published in that PIA.

11 And we said to the public, this is what we're telling
12 our officers, this is how they're conducting
13 themselves.

14 I can certainly take back and look at what
15 we've done with regard to generally, the general
16 inspection policy and see to what extent have we made
17 -- have we reconciled what we say publicly with what
18 we're saying internally. I think that might be.

19 MR. DAVID HOFFMAN: One last problem then
20 I'll be done.

21 I think the other thing that we heard that
22 might be of value then is all that sounds fantastic.

1 If it was told to people that there's a mechanism for
2 making a complaint, where people have gone over that
3 policy and then communicate out, even at an
4 aggregate level, saying, we got so many complaints
5 about how our field agents have performed, and we
6 investigated all of them and we actually took some
7 sort of measure in so many number of those cases -- I
8 think that would provide a lot of confidence from the
9 American people.

10 MR. CASTELLI: We do have a mechanism
11 through the Office of Public Affairs to collect
12 complaints and comments from the public. We say
13 comments because sometimes, oddly enough, people are
14 actually happy with how they were treated, which we
15 always like to note simply because when you give an
16 encouraging word it's nice. But we also, we do take
17 very seriously the complaint process.

18 And we do have several mechanisms for people
19 to basically, what we call Officer Professionalism
20 Complaints. And I think on a large measure, through
21 the 803 process we report out at least on an aggregate
22 metric, those quarterly those complaints.

1 And what we've tried to do more recently
2 under Mary Ellen's guidance, she had asked us to
3 start, can we start flushing out some examples of the
4 types of complaints we're seeing, to give people some
5 context about what we're seeing and what's being
6 looked at. But there is a full process with regard to
7 complaints.

8 It starts as a complaint. If it's reviewed,
9 if it looks to be something that is more serious or if
10 there's corroborating evidence or statements, it'll be
11 referred to Internal Affairs, and then it'll go
12 through an entire discipline process as appropriate.
13 Because CBP does take very seriously its role. You
14 know our officers are law enforcement officers, and
15 they are bound by the law and must follow it as much
16 as they must enforce it. If you're not following the
17 law and enforcing it, then your enforcement's flawed.

18 MR. DAVID HOFFMAN: Thank you very much.

19 MR. CASTELLI: You're welcome.

20 MR. PURCELL: Ramon, please.

21 MR. BARQUIN: You've addressed part of it,
22 but my specific question is if we went back to Detroit

1 today, a year later, when we were there.

2 MS. CALLAHAN: Well, let's do it, Ramon.

3 MR. BARQUIN: First is, would we see a
4 decrease in the false positives that were creating a
5 lot of concern, a lot of disruption in peoples' lives
6 at the minimum level, and some cases really
7 significant harm. So have we seen a decrease first of
8 all. And have we seen an improvement in the redress
9 for those individuals.

10 And third, there were a series of
11 procedures, policies that I understand perfectly the
12 need on the law enforcement side, but the one anecdote
13 that just keeps coming back to me was the CBP officer
14 that said, oh yeah, this individual, third time, we
15 know it's not him, but we still need to go through
16 this process.

17 And it seemed to me that that was some type
18 of a catch-22 that we at this point should know how to
19 fix.

20 MR. CASTELLI: Obviously I would -- yes, I
21 would say you would see a decrease in false positives.

22 I mean, one of the things that we've tried to be more

1 aggressive about -- and you know I'll go right to that
2 third point, is we have TECS, which does the principal
3 screening at the border in terms of lookouts and wants
4 and warrants and that sort of thing. Basically in the
5 end it's a name-based query.

6 And what we've tried to do with it over
7 time, because we recognize that there are these
8 problems of false positives, there's more than one
9 John Smith in this world and John Smith isn't usually
10 the one who's complaining.

11 But what we've tried to do is utilize a
12 travel document, and we have a process that we discuss
13 in the Border Ops PIA. I call it the Border Ops PIA.

14 It's Border Operations Privacy Impact Assessment.
15 And we issued that in the context of the Western
16 Hemisphere Travel Initiative when we were rolling out
17 a number of those documents.

18 The concept I'm talking about is PLOR, which
19 is the Primary Lookout Override. And it's a way that
20 the officers can go into the system and essentially
21 create an override. Because of the way TECS works,
22 because of the fact that whoever's put that lookout in

1 there owns the record, rather than coordinating and
2 going back to them each and every time and say, hey,
3 is this the guy or is this the gal you're looking for.

4 Rather than doing that, once we know, once
5 we know -- I mean the process of the border is you'll
6 be a primary, and if you're a match, you'll get
7 referred to second, where more often than not that
8 match is either resolved favorably because it's a
9 false positive or there's other information that
10 needed to be updated, or it's resolved unfavorably
11 because in fact it's a correct match and there's a
12 reason we need to be talking to you. And I say
13 unfavorably because typically you don't want to have
14 those further conversations.

15 But the point of the Primary Lookout
16 Override is to basically say, if we have gone through
17 that process once, or twice or in your case, three
18 times as you suggested, we don't need to do that
19 anymore. We know that you're not the match to that
20 record.

21 One of the challenges that we're getting
22 better at is, how many other records are there out

1 there that you might also be matching to? Because
2 when we first implemented PLOR, what we discovered was
3 it was great for clearing that one record. But let's
4 say there were four or five records that you matched.

5 We could only clear the one that had initially
6 triggered your referral from primary to secondary.
7 The question then became, how do we go back and how do
8 we get those other records?

9 I would prefer not to have you come through
10 four or five times to hit on each one of those
11 records. And that's what we've worked with and what
12 they've worked with at the National Targeting Center
13 for Passenger, as well as in the Passenger Analysis
14 Units and in field operations generally, are ways to
15 identify those additional records, and to put in the
16 overrides so that once we've determined that the
17 person isn't the proper match and once we've
18 identified a travel document that they're using, we
19 can allow the fact that that travel document is being
20 used a successive time to trigger the override.

21 I mean it's still not perfect because
22 obviously the travel document will trigger the

1 override, but if the inspector looking at the
2 document, looking at the information on the screen and
3 looking at you doesn't think all three compare well,
4 then there'll be -- that referral may still happen.
5 But assuming that it's your enhanced driver's license,
6 and that's the information that's on the screen, then
7 you shouldn't notice that there was even a match to
8 the record.

9 And what we've tried to do is become more
10 aggressive in working both with the trip process at
11 DHS as well as our own internal practices, to use PLOR
12 as a way of essentially eliminating these false
13 positives. Because they take time away from time that
14 could be spent finding people who we're supposed to be
15 spending more time with.

16 MR. BARQUIN: So I gather things have
17 improved?

18 MR. CASTELLI: Yes. My hope is if you go
19 back to Detroit, you'll see that as well. But I know
20 that we've implemented -- I know that there have been
21 some further efforts to in fact implement the PLOR
22 process directly to those secondary records.

1 MR. PURCELL: Thank you. And once again,
2 Lance, take us home.

3 MR. LANCE HOFFMAN: I'll take you home. I'm
4 looking forward to going back to Detroit next year,
5 and I hope when I do, we find something -- there are
6 some good statistics in here. But I'm concerned that
7 they're only in here.

8 I'm back on where David Hoffman was asking
9 the question. I'd love to know about any initiatives
10 you have, either now or in the future, to report back,
11 not only in the ways you do now, but to the affected
12 communities in what might be a more effective way;
13 maybe putting a face on it, whatever.

14 Because seems to me, this message is so
15 muted that the basic idea of whatever you're
16 accomplishing may be getting lost in just the way
17 you're reporting it and not taking it any further.

18 MR. CASTELLI: I think part of what you're
19 talking about is one of the missions of Civil Rights
20 and Civil Liberties. They tend to do a lot more
21 direct outreach with affected communities.

22 I know just recently, we've been working

1 with them as they perform their own Impact Assessment
2 of the border search of electronic devices policies
3 and practices. And I think that is certainly one of -
4 - that is a concern I think that they are raising and
5 that CBP would be working with them more directly to
6 have those outreaches.

7 Because I think given CRCL's position within
8 the Department and their mission to address those
9 concerns in particular, but also, the outreach that
10 they've already done in many respects, with the
11 various communities that can be affected, not the
12 least of which would be the Arab-American community as
13 it relates to in the Detroit area as well as in other
14 areas where we do border searches.

15 I think utilizing them and their Points of
16 Contact is the best way for us to handle that, not
17 only from a CBP perspective but also to allow the
18 department at large to leverage it. Because TSA has
19 screening concerns that can sometimes similarly be
20 implicated as well as ICE.

21 MS. CALLAHAN: So I just kind of -- Larry's
22 talking specifically from the CBP perspective. You

1 said these may be muted, but these are pretty good
2 numbers that are out in the public and were last year
3 as well in the Annual Report, and have as a basis for
4 public affairs comments and so on.

5 With regard to communicating with the
6 community, what we did in Detroit was an exception for
7 our office, because again, we're looking at protection
8 for personally identifiable information. But as Larry
9 pointed out, the statutory responsibility and the very
10 active outreach that CRCL is doing, it is more their
11 bailiwick to kind of communicate that message, while
12 we're talking more about the privacy protections
13 therein.

14 So appreciate it, but also not necessarily
15 the Privacy Office's mission. And as you remember,
16 David Gersten testified on the pending Impact
17 Assessment in December and kind of talked about how
18 our offices obviously are symbiotic but have unique
19 missions.

20 MR. CASTELLI: I mean and we do work with
21 CRCL on these issues as well, so I think naturally
22 there's a way for us to help shape messages, or at

1 least make sure that we're providing them with the
2 information they need to get that message out.

3 MR. PURCELL: Mr. Castelli, thank you very
4 much for your time today. We appreciate your
5 information, and we look forward to seeing you again,
6 so I'm sure we will.

7 MR. CASTELLI: Vegas next time?

8 MR. PURCELL: Yeah, Vegas.

9 MS. CALLAHAN: No, it's not Vegas.

10 MR. CASTELLI: Excuse me? I'll withdraw
11 that thought.

12 MR. PURCELL: Atlantic City?

13 MR. CASTELLI: Detroit. Detroit, they have
14 casinos.

15 MR. PURCELL: This is the moment when as
16 usual we recognize that we have significantly failed
17 to raise any praise, ire or even consciousness from
18 the public as we have no sign-ups for public comments.

19 And so at this point, I would like to
20 announce the conclusion of this meeting, with a
21 reminder that you may submit comments, if you choose,
22 to the Committee at any time by e-mailing them to the

1 e-mail address, PrivacyCommitte@dhs.gov.

2 My thanks to the speakers today, and for
3 your time and for your reports. Very interesting and
4 patience in answering our many questions. This does
5 conclude the public portion of today's meeting, and we
6 are very grateful to our members for participating and
7 for being as engaged.

8 As usual, the transcripts and minutes of
9 this meeting will be posted on the Privacy site of DHS
10 in the very near future, and we encourage everyone to
11 follow the Committee's work by checking that web page
12 frequently.

13 Thank you very much for your time today.

14 [Whereupon, at 11:57 a.m., the meeting was
15 adjourned.]

16

17

18

19

20

21

22