

DEPARTMENT OF HOMELAND SECURITY

- - -

MEETING OF THE

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

- - -

Thursday, December 3, 2009

490 L'Enfant Plaza, S.W.

Room 3207

Washington, D.C.

The meeting was convened, pursuant to notice,  
at 8:37 a.m., RICHARD V. PURCELL, Chairman, presiding.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22

COMMITTEE MEMBERS PRESENT:

RICHARD V. PURCELL, Chairman, presiding

- |                   |                      |
|-------------------|----------------------|
| JOSEPH ALHADEFF   | ANA I. ANTON         |
| RAMON BARQUIN     | J. HOWARD BEALES III |
| JAMES W. HARPER   | KIRK HERATH          |
| DAVID A. HOFFMAN  | LANCE HOFFMAN        |
| JOANNE McNABB     | CHARLES PALMER       |
| NEVILLE PATTINSON | JOHN SABO            |
| LISA J. SOTTO     |                      |

ALSO PRESENT:

MARY ELLEN CALLAHAN, Sponsor and Chief Privacy Officer

MARTHA K. LANDESBURG, Executive Director and Designated Federal Official

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

2 MS. LANDESBURG: We're now going to go on the  
3 record and begin. I am Martha Landesberg, the Executive  
4 Director and Designated Federal Official for the  
5 Department of Homeland Security Data Privacy and  
6 Integrity Advisory Committee. I welcome all of you to  
7 our fourth quarterly meeting of 2009.

8 I'm now going to turn the meeting over to  
9 Richard Purcell, the committee chairman.

10 CHAIRMAN PURCELL: Thank you, Martha. Good  
11 morning, all. I appreciate everybody's attendance at  
12 our meeting this morning of the Data Privacy and  
13 Integrity Advisory Committee.

14 The normal housekeeping rules will apply.  
15 Please, all cell phones, PDAs, and other devices that  
16 will annoy us should be turned off or silenced in  
17 whatever way.

18  
19 Clearly, the audio system is not here, so we  
20 are speaking in our normal voices without  
21 amplification. So I encourage everyone to speak up,  
22 please, and to just try to share your thoughts with the

1 entire room, as opposed to just with your neighbors.

2 We also have time on our schedule at 11:45  
3 for public comments. So those members of the public  
4 who are interested in addressing the committee at that  
5 time, please use the sign-in. Martha, where is our  
6 sign-in sheet for the public?

7 MS. LANDESBURG: It's out in the main  
8 reception room.

9 CHAIRMAN PURCELL: Outside this room, which  
10 is what my notes say.

11 At this time I'd like to welcome Mary Ellen  
12 Callahan, the Chief Privacy Officer for the Department  
13 of Homeland Security, to our meeting. Ms. Callahan  
14 prior to joining the Department specialized in privacy,  
15 data security, and consumer protection law as a partner  
16 at Hogan and Hartson, LLP, here in Washington, and has  
17 served as the Co-Chair of the On-Line Privacy Alliance,  
18 a self-regulatory group for industry.

19 She also has served as the Vice Chair of the  
20 American Bar Association's Antitrust Division Privacy  
21 and Information Security Committee; and, together with  
22 the data privacy team here in the Department, Ms.

1 Callahan is responsible for compliance for privacy  
2 across all of DHS and its components and serves as the  
3 Department's chief Freedom of Information Act Officer.

4 Mary Ellen, please proceed.

5 DHS PRIVACY OFFICER UPDATE,

6 BY MARY ELLEN CALLAHAN

7 MS. CALLAHAN: Thank you, Mr. Chairman.

8 I want to welcome all of the committee  
9 members here today. I also want to welcome the members  
10 of the public who have joined us.

11 I wanted to acknowledge that this is the  
12 first DPIAC meeting that we are having specifically  
13 under the Secretary's efficiency review process. The  
14 Secretary has looked at many ways of having the  
15 Department be more efficient, including the use of  
16 renting hotel spaces and other spaces when there's good  
17 federal spaces available as well. So I wanted to thank  
18 GSA for working with us to find a space for DPIAC today  
19 here in Washington, and I wanted to thank the committee  
20 members for finding the space GSA found for us.

21 (Laughter.)

22 We recognize it was a little difficult to

1 find initially, but at the same time I think it's  
2 important to adhere to the Secretary's efficiency  
3 standards and I think it's an important one to utilize  
4 federal space as we can.

5 So I wanted to start with giving an overview  
6 of the activities of the office since we last met in  
7 Detroit in September, on September 10th. As usual,  
8 there is a lot going on, so there's a lot of things. I  
9 will try not to bore you, but also give you the  
10 highlights of what my office has been working on.

11 In addition, in keeping with the theme of the  
12 support that the committee is going to be providing to  
13 us today, we're going to be focusing on the  
14 Department's engagement with the public during the  
15 meeting today. So first we're going to hear from my  
16 colleague Rose Bird, who is our Director of Privacy  
17 Incidents and Inquiries. She's going to give a  
18 briefing on our new complaint tracking system, as well  
19 as the Privacy Office's role with the DHS traveler  
20 Redress Inquiry Program, as well as providing an update  
21 on her group's activities, the privacy incidents and  
22 inquiries reports. So she'll do that in lieu of me

1 providing the update for her.

2 We'll next hear from Patty Cogswell, who is  
3 the Acting Deputy Assistant Secretary and Executive  
4 Director of the Department's Screening Coordination  
5 Office. Patty's going to talk a little bit more about  
6 her office's role in developing Department screening  
7 programs.

8 David Gersten, Acting Deputy Officer for  
9 Programs and Compliance in the DHS Office for Civil  
10 Liberties and Civil Liberties, and somebody who has  
11 worked very closely with me since I came on board in  
12 March, will then discuss his office's work on a civil  
13 liberties impact assessment for DHS border searches  
14 of electronic devices.

15 As I mentioned, in general there are many  
16 exciting developments that are taking place for the  
17 Privacy Office. I wanted to start first with the big  
18 picture view of some of the policy issues that the  
19 Department is involved with, go across the pond, so to  
20 speak, and then bring it back home to the Department's  
21 work.

22 Some of the policy issues that we are working

1 on in our office. We have just released a report  
2 summarizing our public workshop on Government 2.0,  
3 Privacy and Best Practices. It was a conference that  
4 took place in June, very well attended, I think very  
5 useful. It was the first government conference  
6 addressing issues of social media, particularly by the  
7 government. As we all know, the president has asked the  
8 government to think about ways to be more creative with  
9 utilizing social media when interacting with the  
10 public.

11 The report I think did a great job of  
12 summarizing the tensions of those issues, both the  
13 legal issues, policy issues. As many of you know, I  
14 formerly was a social media privacy lawyer, and when I  
15 came to DHS I thought it was going to be a piece of  
16 cake. I was like: I know this stuff; not a problem.  
17 And then you layer on top of it the First Amendment and  
18 records retention and all different things like that  
19 and suddenly you have got a very interesting question.  
20 I think that this report does a great job of  
21 summarizing it. It is, as all of our reports are,  
22 available at [dhs.gov/privacy](https://dhs.gov/privacy). But we've gotten a lot

1 of compliments from our inter-agency partners that this  
2 is a useful tool as well.

3 Speaking of inter-agency partners, as you  
4 know, I serve as the Co-Chair of the Federal CIO  
5 Council's Privacy Committee. That privacy committee is  
6 the first committee in which the federal privacy  
7 professionals can get together and talk about policy  
8 issues in a collaborative way. I wanted to personally  
9 thank Toby Levin for her leadership on helping work out  
10 a lot of the best practices within the committee  
11 throughout the year.

12 In October the Committee itself sponsored its  
13 second annual privacy summit for federal privacy  
14 officials. It was paired with the IT summit for the  
15 CIOs for the IT professionals, and several Privacy  
16 Office staff members and I participated in a panel. It was  
17 well attended and there were over 500 federal employees  
18 who were there, which is a great turnout and, not to be  
19 competitive, more than the IT summit. I'm just saying.

20 (Laughter.)

21 I specifically mentioned Toby and her work  
22 with the Privacy Committee. Several other office

1 members have been participating in several different  
2 elements of the Privacy Committee itself throughout the  
3 year and I wanted to thank them, including for Web 2.0  
4 privacy issues, working on terms of use, helping define  
5 privacy principles for federal enterprise architecture,  
6 as well as working on defining best practices with  
7 international privacy policy.

8           So we've been very active on the inter-agency  
9 work to try to really leverage best practices from all  
10 the departments across the board.

11           Then finally on the policy side, we are also  
12 working on a guide to describe how our office  
13 carries out its duties and responsibilities, a bit of a  
14 primer on the Privacy Office. I've had conversations  
15 with some of my inter-agency colleagues saying: How'd  
16 you do it? How did it work, and what's going on?  
17 We're working on having a little kit on the things that  
18 DHS is working on and that will be available in spring  
19 of 2010.

20           Next we're going to take a small journey  
21 during this update and talk a little bit about  
22 international privacy policy work that we've been

1 doing. We've been extraordinarily busy on the  
2 international front since the Committee last met. On  
3 October 28th the Department of Homeland Security, along  
4 with the Departments of Justice and State, the European  
5 Union Presidency, and the Vice President of the  
6 European Commission announced the completion of the  
7 High Level Contact Group principles. As you may  
8 recall, these data protection principles are the  
9 culmination of nearly 3 years of work.

10 The principles themselves are a standard by  
11 which they were to acknowledge that the United States  
12 and the European Union have similar approaches to data  
13 protection issues. They're essentially, I'd say, the  
14 FIPPs on steroids, really drilling down on several  
15 issues associated with data protection, specifically in  
16 the law enforcement and national security arena.

17 Although the principles themselves are not a  
18 binding agreement, they certainly will be part of  
19 future information-sharing agreements between the EU  
20 and the U.S. Then the ultimate goal is not only to  
21 have a binding agreement with the EU and the U.S. on  
22 law enforcement issues, but also to raise the standard

1 for information-sharing in the law enforcement and  
2 security context throughout the world. So hopefully  
3 that will work as well.

4 This fall -- we were talking about the fall  
5 and the trip to Europe -- we also had John Kropf, my  
6 deputy, and Lauren Saadat, one of the international  
7 privacy directors and I attended the EU-U.S. high-level  
8 contact group redress workshop and subsequent experts  
9 group meeting in Brussels in the beginning of October.  
10 The purpose of the workshop was to finalize the  
11 language on effective redress and to work together to  
12 try to acknowledge what are principles associated with  
13 effective redress.

14 I also have met with members, several members  
15 of the LIBE Committee, which is of course the European  
16 Parliament's Committee on Civil Liberties, Justice, and  
17 Home Affairs, to discuss the privacy impacts of DHS  
18 programs, the U.S.-EU PNR joint review, which will take  
19 place next year, and of course the role of the DHS  
20 Privacy Office.

21 In November, as many of you know, I was able  
22 to travel to Madrid, Spain, with Secretary Napolitano.

1 She was a keynote speaker at the International  
2 Conference on Data Protection and Privacy  
3 Commissioners. She and her Spanish counterpart were  
4 among the first data owners, actually, to speak to the  
5 data privacy group since the program started over 30  
6 years ago. I think it was a useful exchange to  
7 acknowledge the different approaches to data, to data  
8 usage.

9 I also then accompanied the Secretary on her  
10 travels to London and Brussels for additional meetings  
11 with officials from several EU member countries and the  
12 European Parliament concerning information-sharing.  
13 Privacy and security were primary topics throughout  
14 those meetings.

15 Here in Washington, the Privacy Office hosted  
16 -- as a matter of fact, the Privacy Office hosted two  
17 EUROPOL representatives and a representative from the  
18 French Data Protection Authority, the CNIL, who  
19 focuses on law enforcement issues, as part of our  
20 ongoing series of information exchanges with our  
21 international counterparts. I specifically want to  
22 thank our new international privacy colleague, Nicole

1 McGhee, who's over my right shoulder, for having joined  
2 the office, I believe in August. She helped put  
3 together this program and was the coordinator for the  
4 whole event. So I wanted to thank her for her work,  
5 and also to thank members of my office as well as  
6 privacy professionals throughout the government for  
7 supporting our goal to engage in an exchange of best  
8 practices to learn about the U.S. privacy framework.

9           We are, going forward, going to probably have  
10 this type of exchange twice a year and have  
11 worked with law enforcement privacy professionals in  
12 Europe and actually throughout the world to try and  
13 have, as I said, a multilateral exchange on these types  
14 of issues. We have indeed had Canadian and Mexican  
15 participants in the past, as well as representatives of  
16 several European countries.

17           In addition, the Safe Harbor Conference was  
18 last year and I was able -- my office was able to meet  
19 with several of the data protection administrators who  
20 were here as part of that.

21           In addition to the international work that  
22 we've been working on, there are several new activities

1 on the legislative and regulatory front specifically  
2 with regard to fusion centers. The Privacy Office  
3 continues to be deeply involved in the Department's  
4 work on fusion centers to make sure that privacy  
5 protections are in place. In fact, the office has  
6 increased its role in that type of work in the past few  
7 months.

8 The Secretary recently called for the  
9 establishment of a new DHS Joint Fusion Center Program  
10 Management Office, which acronym is JFC-PMO, and I just  
11 call it the J-F-P-something-something-something,  
12 because it's way too long. But the JFC-PMO is within  
13 the Department and it is specifically charged with  
14 increasing the effectiveness and oversight of the  
15 fusion center program. Protecting privacy and civil  
16 liberties is one of the seven specific goals the  
17 Secretary articulated for the JFC-PMO.

18 I sit on the DHS committee assembled to draft  
19 the concept of operations plan, as well as the  
20 implementation plan of the JFC-PMO. Furthermore, we  
21 co-chair the subcommittee on privacy and civil  
22 liberties, we'll staff the training committee and the

1       subcommittee examining fusion center baseline  
2       capabilities, which of course include privacy  
3       requirements. Among those who are helping to staff  
4       those things are our own Martha Landesberg, the  
5       Executive Director for your Committee, but also a jack  
6       of all trades on assisting us with these types of  
7       developments.

8               The JFC-PMO at DHS mirrors a government-wide  
9       effort to establish a national program management  
10      office for fusion centers. I am also a member of the  
11      inter-agency management group that oversees that and  
12      co-chair along with my colleague from the Department of  
13      Justice, Nancy Libin, the subcommittee dedicated to  
14      privacy and civil liberties in that regard.

15             Speaking of fusion centers, the Privacy  
16      Office continues to support fusion centers as part of  
17      the Information-Sharing Environment and in fact has  
18      begun to increase its role and oversight in the privacy  
19      elements of fusion centers. As we all know, the  
20      Privacy Office has a statutory requirement to do  
21      privacy assessments on fusion centers. The first one  
22      was done in December of 2008 prior to my arrival, and

1     what it said is basically privacy protections needed to  
2     be in place in fusion centers, and that hopefully will  
3     take place in the future.

4             What my office has done, in collaboration  
5     with the Information-Sharing Environment Office, is to  
6     do several things with regard to working with fusion  
7     centers to increase their awareness and recognition of  
8     privacy protections. First, of course, we are engaging  
9     in privacy training for I&A analysts. That's been  
10    ongoing. We've also been working with our partner  
11    CRCL working on training for fusion centers. We're  
12    also trying to leverage additional privacy training  
13    through other sources who are working with fusion  
14    centers.

15            But more importantly, we're working with the  
16    fusion centers themselves to have them finalize and  
17    conclude their own privacy policies, which are required  
18    under the Information-Sharing Environment. To date,  
19    only a handful of privacy policies have been made  
20    public, have been finalized and been made public.

21            In the summer I spoke with the Information-  
22    Sharing Environment program manager and I said, we need

1 to move this along. The Department of Homeland  
2 Security, given its role with fusion centers, I offered  
3 our office to help review all of the privacy policies  
4 and to make sure that they are -- to confirm that the  
5 fusion center privacy policies are at least as  
6 comprehensive as the PMISC's privacy guidelines. That  
7 phrase "at least as comprehensive" is from the fusion  
8 center guidelines. We are not fly-specking the  
9 policies. We are not line editing the policies. But  
10 we are making sure that they have the basic privacy  
11 principles associated with an information-sharing  
12 environment. So that will be -- that's an ongoing  
13 process.

14 In addition, we are -- I can say this  
15 publicly -- we are looking at encouraging people to  
16 conclude privacy policies at the fusion centers in the  
17 near future, and on Monday we will be able to give you  
18 publicly more information about that encouragement. So  
19 we'll put a place-holder there.

20 So I think that that will be a useful  
21 mechanism. In addition, for the centers that do  
22 already have completed privacy policies or almost

1 completed privacy policies, we're going to look at  
2 having privacy impact assessment training for those  
3 fusion centers so they can do their own analysis of  
4 what the privacy impacts are of the fusion centers and  
5 of the information-sharing, and that effort will be led  
6 by Ken Hunt and my special assistant Lynn Parker for  
7 the next calendar year.

8           Maybe, quite frankly, that may be premature.  
9 But we're going to see and we're going to hope that  
10 that will be useful for those more advanced fusion  
11 centers.

12           Briefly on some technology and intelligence  
13 issues. As some of you know, we have completed a  
14 penultimate draft of a classified PIA on the next  
15 iteration of the Department's cyber security work, also  
16 known as "the Exercise." My Director of Privacy and  
17 Technology Intelligence, Pete Sand, and I are working  
18 on providing a comprehensive unclassified version of  
19 the PIA, and that will take place prior to the launch  
20 date of the Exercise performance itself.

21           Relatedly, I also have been actively  
22 participating in a sub-inter-agency policy committee

1       which is on -- there's an inter-agency policy committee  
2       on cyber security.  There's a sub-IPC on privacy and  
3       civil liberties, and the Department of Homeland  
4       Security both on the CRCL and privacy side have been  
5       leaders in that dialogue of cyber security privacy  
6       issues on a policy level.  And Pete has been  
7       actively participating in the privacy summit and in  
8       other public forums discussing privacy protections and  
9       the Federal cyber security effort.

10               I want to talk a little bit about compliance  
11       and what our compliance team has been working on  
12       since September.  The group since September has  
13       approved 135 PTAs, Privacy Threshold Assessments, 21  
14       Privacy Impact Assessments, and 7 System of Records  
15       Notices, since September.

16               We also have some good news on the FISMA  
17       front.  Our annual FISMA reporting period closed in the  
18       beginning of October.  The Department improved its SORN  
19       score from 90 percent in FY '08 to 93 in FY '09.  DHS  
20       has improved its PIA score from 48 in FY '08 to 67 in  
21       FY '09.  Our goal that I've set for Becky and her team,  
22       which they of course will meet, is to score above 80

1 percent by the end of fiscal year 2010. I think that's  
2 an achievable goal.

3 I particularly wanted to recognize and thank  
4 Lyn Rahilly, who has been the ICE Privacy Officer since  
5 April 2008, for her efforts. Since Lyn's been on the  
6 job, the ICE PIA FISMA score has improved from 31  
7 percent in '08 to 51 in '09, and the SORN score rose  
8 from 83 to 88. She's really working on getting a lot  
9 of backlogged processes moving forward, as well as  
10 being part of the policy development within ICE itself.

11 We are also working on the compliance team on  
12 the first DHS-wide Privacy Impact Assessments on the use of  
13 social media. The PIAs that we are going to work on --  
14 we're going to work on four different buckets of PIAs.  
15 One we're working on essentially for video and image-  
16 based social media applications, so in colloquial  
17 terms, YouTube, and having a Privacy Impact Assessment  
18 for Flickr, YouTube, and other things where it's  
19 primarily images that are being transmitted and being  
20 displayed and being presented.

21 We're simultaneously working on Department-  
22 wide Privacy Impact Assessments for social networking

1 tools involving a more social collaboration. By  
2 that I mean Facebook, MySpace, and so on. We're also  
3 going to work on a Privacy Impact Assessment for  
4 applications, for the use of applications, if need be.

5 We of course in early August had a Privacy  
6 Impact Assessment specifically for the use of the DHS  
7 site, ourborder.ning.com, which was -- it's a social  
8 media micro-site for collaboration on Southwest border  
9 issues, as well.

10 The compliance group has also been  
11 participating in the e-authentication working group, an  
12 inter-agency initiative to draft a model PIA that will  
13 provide guidance to Federal agencies for the use of  
14 federated identity solutions. That is actually part of  
15 the Privacy Committee work that I mentioned previously.  
16 The Privacy Committee is going to have identity  
17 management as one of its subcommittees for next year  
18 and work collectively with the CIO council and with  
19 others who are addressing these issues, addressing  
20 these issues on a Federal level.

21 Another aspect the compliance group has done  
22 to further leverage our relationship with the Chief

1 Information Office: group members have been  
2 attending a number of the IT program reviews that have  
3 been initiated by the new CIO, Richard Spires, who has  
4 been a great partner already. This participation by  
5 not only the compliance group members, but also by  
6 component privacy officers, has been a great way to  
7 gain insights into DHS's major IT investments and to  
8 hone the team's ability to spot potential privacy  
9 issues in the systems. So I think that that's been a  
10 great collaboration both at the component level,  
11 because the Privacy Office was there, and our  
12 compliance team as well.

13 Our agenda for next year for the compliance  
14 group is, in addition to obviously our ongoing work  
15 with PTAs, PIAs, and SORNs, is to work with the CIO,  
16 I&A, the Screening Coordination Office, who you'll hear  
17 from later, and the components, to try to develop a  
18 privacy-sensitive framework for assuring that when a  
19 domestic threat arises DHS is able to effectively,  
20 efficiently, and appropriately search its databases in  
21 both a classified and unclassified setting.

22 Another initiative that we're taking on that

1 is one that I had as a significant goal when I first  
2 took this job in March is to update our PIA guidance  
3 and template to make sure that we're being clear with  
4 our privacy analysis and making sure that the PIA  
5 itself is more effective, efficient, and, quite  
6 frankly, user-friendly.

7 We have been working with the components to  
8 also give feedback associated with this revision of the  
9 PIA. We hope to roll that out fairly early next year.

10 As Richard mentioned, I am also the Chief  
11 FOIA Officer, and I just wanted to note some things  
12 that are going on in the FOIA world. As you may recall  
13 from our September meeting, in late August I issued a  
14 proactive disclosure memo for the Department asking all  
15 of the components, to the best of their ability,  
16 to proactively disclose categories of information on  
17 the electronic reading room sites or on the DHS FOIA  
18 site itself.

19 The categories of records that are expressly  
20 identified Department-wide include: historical daily  
21 schedules for senior officials, awarded contracts and  
22 grants awarded, management directives and instructions,

1 Congressional correspondence under DHS control, FOIA  
2 logs, and then all other records that the component may  
3 identify that would be typical types of frequently  
4 asked records, for the components themselves to have  
5 some discretion there.

6 We've issued some follow-up guidance on the  
7 proactive posting of senior officials' calendars and we  
8 have indeed posted records, the calendars, the  
9 historical calendars of the Secretary, myself, as well  
10 as several other senior officials already. We have  
11 posted all of the FOIA logs since the Department was  
12 stood up. We've produced several dozen management  
13 directives, several dozen contracts.

14 The component FOIA officers have been working  
15 very diligently on their side as well to get this  
16 information -- first it's got to be made 508-compliant  
17 and so it's taking a big process of loading that up to  
18 be consistent with the ADA. But at the same time,  
19 we've been making great strides with that since August,  
20 and in fact this has been identified by other FOIA  
21 officers throughout the federal government as a real  
22 initiative. Some of my colleagues were at several FOIA

1 conferences this week where DHS was exhibited as a role  
2 model on its proactive disclosure to have the  
3 information that is frequently requested or may be  
4 requested or is often requested, make it available now,  
5 so that we can make it be part of our transparency and  
6 be consistent, not just with the President's express  
7 mission, but obviously our requirement as federal  
8 officials.

9 I have some administrative responsibilities  
10 with FOIA right now. We have our FY 2009 annual FOIA  
11 report to the Attorney General. That's due in January.  
12 Then I've also been instructed to have my first Chief  
13 FOIA Officer Report, which is new Attorney General  
14 guidance, and that is due in March.

15 Then I just wanted to close with some good  
16 news, which is I had foreshadowed some important  
17 hiring that's going to be taking place. We are  
18 finalizing a few other positions, so hopefully I'll  
19 have news in our next meeting. But we were since we  
20 last met able to hire two new Associate Directors for  
21 Compliance, who will focus on standardizing the  
22 compliance processes, enhancing the quality of

1 compliance documentation, implementation of privacy by  
2 components, working directly with the components, and  
3 then again at my request to work on some back-end  
4 review and oversight of the privacy process for the  
5 previously posted Privacy Impact Assessments and System  
6 of Records Notices.

7 In addition, we've just hired a new Associate  
8 Director for Communications and Training, Steve  
9 Richards, who has hit the ground running, and his  
10 portfolio will include the Privacy Office's web site,  
11 which I hate. I think it needs to be updated and be  
12 much more user-friendly, and he knows that and he  
13 agrees. We're also working with him on outreach  
14 materials, privacy training courses, and materials for  
15 headquarters staff and components.

16 So we're really excited. It's been a great  
17 calendar year. It's been a great 8 months for me  
18 personally. So I wanted to thank the Committee for  
19 their attention, and I open it up to questions if  
20 that's okay with the Chairman.

21 CHAIRMAN PURCELL: Of course. Thank you,  
22 Mary Ellen. I appreciate that.

1           Are there questions? Neville, let's start  
2     with you.

3           MR. PATTINSON: A very busy few months, Mary  
4     Ellen, and thank you for your report. I appreciate  
5     that.

6           I just wanted to ask a question. We had a  
7     visit to a fusion center in Las Vegas, I think it was.

8           MS. CALLAHAN: Is that what the reason for  
9     the trip was?

10          MR. PATTINSON: I believe it was El Paso as  
11     well.

12          One of the questions I have is really about  
13     the JFC-PMO activities. Obviously, a lot of good work  
14     going on there with the PIAs and the whole privacy  
15     awareness going on. Is this actually changing the  
16     practices, do you know, within the fusion centers, or  
17     is it awareness that we're really putting into the  
18     people that are in the fusion centers? Are we making  
19     an impact in actually how they change their operational  
20     day to day practices, or is it just --

21          MS. CALLAHAN: I think it's both. I do think  
22     it's both, and I think that it's not just the JFC-PMO,

1 but it is also the training that we have done  
2 collaboratively with the Office of Civil Rights and  
3 Civil Liberties. They have taken the laboring oar on  
4 this training, quite frankly. But we have privacy  
5 modules and it's a lot of really -- the fusion centers  
6 are hungry for it and hungry for understanding this  
7 scenario and what they can and cannot do.

8 So I think it is both of those, both in terms  
9 of our goals as well as in terms of hopefully the  
10 actual results.

11 MR. PATTINSON: Good.

12 CHAIRMAN PURCELL: John.

13 MR. SABO: Mary Ellen, you didn't  
14 specifically mention cloud computing, which is of  
15 course at the top of everyone's agenda. But it's  
16 certainly being promoted by the administration. I'm  
17 wondering if the office, your office, has begun to  
18 either work with NIST on some of the privacy  
19 implications -- could you just talk about what your  
20 involvement is with cloud computing privacy issues?

21 MS. CALLAHAN: Absolutely. In fact, if you  
22 want to come to the Privacy Committee meeting later on

1 today, we're going to talk about that. It's a great  
2 question, John. Cloud computing obviously is a very  
3 important issue and needs to be done properly.

4 The Privacy Committee, as I mentioned, which  
5 is a subcommittee, it's a sub-group of the CIO Council,  
6 for its FY 2010 has as -- we created a joint Web 2.0  
7 cloud computing committee, because I think several of  
8 the issues overlap. There are several that are  
9 obviously discrete in each of those. There had been a  
10 smaller working group of people, including  
11 Toby, working on cloud computing issues on some of the  
12 smaller groups within the CIO Council and a parallel  
13 committee. There's a cloud computing committee under  
14 the CIO Council and people have been working with that.

15 We're going to hopefully formalize that more  
16 at today's meeting and talk about how the federal  
17 privacy professionals could be involved in that  
18 dialogue more formally and with larger breadth in 2010.  
19 I think that's very important for us, to make sure that  
20 if we can be involved we will be involved.

21 There are obviously other conversations on  
22 cloud computing, not just the CIO Council, but we're

1 aware of those types of things, but are trying to  
2 leverage our relationships with the CIO Council and  
3 with other equities to make sure that we are -- that  
4 privacy professionals, not just the DHS Privacy Office  
5 of course, aren't spread too thin, but are engaging at  
6 the appropriate times.

7 CHAIRMAN PURCELL: So I'd like to go to Joe  
8 next and then Ramon.

9 MR. ALHADEFF: Thank you.

10 It does sound like a very busy few months.  
11 You had mentioned a PIA on some of the social  
12 networking applications, the first tranche being the  
13 more video or image-oriented ones. I was just  
14 wondering, because when industry has been looking at  
15 these issues they look at both how you're able -- how  
16 you're allowed to use them in terms of what you may  
17 post and how you may use it, as well as what you may  
18 source from it. I was just wondering if the PIA was  
19 looking at both of those aspects or was focusing only  
20 on one or the other.

21 MS. CALLAHAN: The question is whether or not  
22 we're doing kind of, what I say is we set up a

1 storefront and people come in or whether somebody else  
2 sets up a storefront and we go in. We're talking more  
3 about DHS setting up the storefront, what the rules of  
4 the road are for that. Those are ones we've been  
5 working with the Office of General Counsel and with the  
6 Office of Public Affairs, of course, as well as our  
7 security officers, to make sure when we set up our  
8 storefront that we do so consistent with all laws, with  
9 all security issues, as well as making sure that there  
10 is a process.

11 So we have a draft process to make sure that  
12 that's working. Several of the components, including  
13 TSA, have been real leaders on the social media issues.  
14 But so for us, we're doing it that way.

15 With regard to when somebody else sets up a  
16 storefront and we go in, if we were to engage in that  
17 activity we would do a PIA.

18 CHAIRMAN PURCELL: Thank you.

19 Ramon.

20 MR. BARQUIN: Mary Ellen, I will echo my  
21 colleague's congratulating you on the amount of  
22 activity that you've been engaged in. It's sort of my

1 official role as nudge on what of the issues that we as  
2 a committee at least are supposed to tackle. I just  
3 wanted to ask you, do you have any plans to deal with  
4 data integrity at all as a necessary prerequisite  
5 even before privacy?

6 MS. CALLAHAN: I think you guys are reading  
7 the notes that I didn't read on my presentation, you and  
8 John both. In fact, I appreciate your hard work on  
9 the data integrity issues and we are working on that in  
10 several ways. I do have a requirement. There's a DHS  
11 Data Integrity Board specifically that is required, and  
12 the compliance group did have on their list of  
13 activities that they need to accomplish to formalize  
14 the structure and activities of the Data Integrity  
15 Board. I skipped over it because I missed it.

16 So that's part of kind of the formal  
17 structure, but that I think also plays into the  
18 conversation that I mentioned in terms of the effective  
19 and appropriate searching during threat stream  
20 scenarios. It's a similar phenomenon and does  
21 percolate a lot to the compliance work as well as the  
22 policy, technology, and intelligence groups.

1           CHAIRMAN PURCELL: Lisa.

2           MS. SOTTO: Thank you.

3           Thank you, Mary Ellen. It's such a pleasure  
4 to serve with you.

5           With respect to the Madrid conference, it's  
6 always been kind of a puzzle for the Europeans that we  
7 don't have in the United States an independent data  
8 protection authority. I think it's just fantastic that  
9 you and the Secretary went over there and were formally  
10 invited to speak. That's a big move forward, I think.

11           Do you think that criticism is still being  
12 levied or do you think your presence there has really  
13 mitigated that criticism?

14           MS. CALLAHAN: Well, I think it is -- I think  
15 there are two very different structures that -- there  
16 are several ways to try to have effective and  
17 operationalized privacy. The Europeans have chosen one  
18 style. The Congress has not chosen to have that same  
19 style for the Executive Branch. I think there's always  
20 going to be some tension there.

21           In my conversations with the Europeans,  
22 although they recognize that my office has done a lot

1 of good work, they still see me as beholden. One  
2 example I gave -- Jim knows this; I gave this example a  
3 couple weeks ago, which is, there are pros and cons to  
4 both types of scenarios. I'll use advanced imaging  
5 technology, whole body imaging, as an example, which I  
6 did at the Privacy Coalition 10 days ago. I met with  
7 the Dutch DPA the day before and we talked about whole  
8 body imaging, and they said: Yes, we have it at  
9 Schiphol and the person who is walking through -- as you  
10 guys know; we did it in Detroit. The person walking  
11 through the meter can look up and see, yes, that's  
12 Joan, she's walking through, I see what she looks like.  
13 There's no masking of the face, there's none of the  
14 privacy protections that our TSA Privacy Officer and  
15 our office were able to get implemented because we are  
16 part of the privacy policy process.

17 Mr. Kohnstamm said: You guys did it better,  
18 you guys absolutely did it better, because you were  
19 part of the process. So it depends on how -- where you  
20 want to be effective and where you want the fights to  
21 be.

22 I think I've said this to you guys

1 informally. I'd much rather be in the cabin of the  
2 shipliner and say, "That is an iceberg; turn," as  
3 opposed to come up afterwards and say, "Yes, we hit an  
4 iceberg." So it's a little bit of a process. Is it  
5 after-the-fact review or is it proactive, trying to  
6 anticipate the scenarios? You may hit an iceberg or  
7 two, but hopefully not all of them, given that you're  
8 in the cabin with them.

9 But I think there's going to be that tension  
10 all the time. Hopefully, we'll mitigate some of it,  
11 but it'll still be there. But they have a  
12 parliamentary system, too, and it's a very different  
13 scenario. They keep saying, why can't you do X and Y.  
14 I'm like: Go down the street and talk to Congress.

15 CHAIRMAN PURCELL: You say that politely,  
16 right?

17 MS. CALLAHAN: I say that politely all the  
18 time.

19 CHAIRMAN PURCELL: Annie.

20 MS. ANTON: So thank you very much for a  
21 report about a lot of things and a very productive time  
22 in the office. We appreciate your efforts.

1           I was wondering -- and a realize you may not  
2   be able to answer this, but if that's the case that's  
3   fine. I was wondering if there's anything that you can  
4   say about the cyber Exercise before the public PIA? If  
5   you can't, that's fine. But I was just curious if  
6   there was something you could say.

7           MS. CALLAHAN: There is public affairs  
8   guidance on the Exercise. I do not have it  
9   internalized yet. There's a lot of work that's being  
10  done. I can say that the Department is finalizing an  
11  unclassified white paper about the Exercise  
12  specifically, trying to make it detailed, to address  
13  several of the public questions about the Exercise that  
14  have been raised since July, but also to do so in an  
15  unclassified way. That is --

16          MS. ANTON: Is it possible to say who is  
17  involved, who participated, or not, or who is  
18  participating?

19          MS. CALLAHAN: The agencies who are  
20  participating or the people?

21          MS. ANTON: Agencies.

22          MS. CALLAHAN: That is part of the

1 classification issue.

2 MS. ANTON: No worries.

3 MS. CALLAHAN: So we are strongly hoping that  
4 that participation can be put forward.

5 MS. ANTON: Thank you.

6 MS. CALLAHAN: That is outside of the  
7 Department's hands, though.

8 MS. ANTON: I understand.

9 MS. CALLAHAN: That's at a higher level.

10 CHAIRMAN PURCELL: For myself, I'd like to  
11 just make a comment on the international coverage. I  
12 know you've been very busy, and I think most of the  
13 committee members, myself in particular, are very  
14 grateful for having the outreach effort. We know that  
15 privacy is a globally affecting issue and that American  
16 commerce and much of our economic strength rests on  
17 free trade and the free flow of data. So having good  
18 relationships with our European neighbors, particularly  
19 in privacy, is very important to us all.

20 Part of the High Level Contact Group's  
21 conclusions was based on continuing disagreement,  
22 though, which is on redress. Redress procedures are

1 something that the committee is taking up, and I want  
2 to remind all of the Committee members that focus on  
3 this issue is going to be very, very important. I  
4 personally am looking for a resolution from the  
5 Committee before long, and they know that, for guidance  
6 in redress.

7 We think that this is a critically important  
8 issue to move forward, to demonstrate to our European  
9 colleagues that we are serious, legitimate players in  
10 this, and despite our differences we have an approach  
11 that is effective as well. We have to demonstrate  
12 that.

13 So my comment is: Committee members, one of  
14 the things we haven't talked about here is redress  
15 procedures. We'll hear from Ms. Bird soon about the  
16 progress in the Department around that. We as a  
17 Committee need to make progress on that as well to help  
18 provide guidance to the office.

19 That's a mere comment, but I look forward to  
20 a conclusion on this issue before long.

21 Thank you, Mary Ellen, very much for your  
22 time today. We appreciate it.

1 MS. CALLAHAN: Thank you.

2 CHAIRMAN PURCELL: The update was terrific.

3 Now, we have with us today -- it's our great  
4 privilege to welcome Rose Bird. Rose is the  
5 Department's -- the Privacy Office's first Director of  
6 Privacy Incidents and Inquiries. Rose has perhaps the  
7 unenviable responsibility for investigating privacy  
8 complaints that are received throughout the Department,  
9 including those complaints that are received from the  
10 general public, from nonprofit organizations, and from  
11 self-regulatory organizations.

12 She's also responsible for the privacy  
13 incident management program in the Department and  
14 collaborates in that with the Enterprise Operations  
15 Center, component privacy officers, with the privacy  
16 points of contact in components, and also with DHS  
17 management. So in this capacity Ms. Bird is  
18 essentially tasked with ensuring that privacy incidents  
19 are: first, properly reported; second, mitigated; and  
20 that remediation efforts are appropriate for each and  
21 every incident.

22 We look forward to your comments, Ms. Bird.

1 DHS PRIVACY OFFICE COMPLAINT TRACKING SYSTEM,  
2 BY ROSE BIRD, DIRECTOR, PRIVACY INCIDENTS AND  
3 INQUIRIES, DHS PRIVACY OFFICE

4 MS. BIRD: Thank you. Thank you for having  
5 me. I've been here exactly a year. I came here before  
6 Thanksgiving and I met many of you on a subcommittee,  
7 so it's great to be back speaking from a position of  
8 somewhat authority. But I am the Privacy Incidents and  
9 Inquiries Director, as mentioned.

10 You've got your slides. You can follow  
11 along. I've just got an agenda. I'm going to speak  
12 about my position and I'll give you an update which is  
13 not part of the slide presentation, on what we've been  
14 doing on incidents and inquiries. And since you're  
15 interested in redress, I'll talk about the Complaint  
16 Tracking System and our role in DHS.

17 Hard copies are available outside for anyone  
18 who wants to grab one.

19 (Pause.)

20 CHAIRMAN PURCELL: I think you can go ahead,  
21 Rose. It's fine.

22 MS. BIRD: If you want to just follow along

1 with your slides. As mentioned, I'm the Director of  
2 Incidents and Inquiries. Our acronym is "PIIG," P-I-I-  
3 G, unfortunately. So we do feel like -- we have a  
4 staff of three. I have two teammates and we feel like  
5 we are the three little pigs trying to keep the wolf at  
6 bay.

7 The position was established in October and  
8 I've got two roles: investigating privacy complaints  
9 and incidents also. Most of you know that incidents  
10 are the breach of information, when personally  
11 identifiable information is released. So a complaint  
12 may become an incident, so that the two are  
13 interrelated often.

14 I am mandated to minimize and prevent privacy  
15 incidents in accordance with the responsibilities of  
16 Section 222 of the Homeland Security Act and the  
17 Privacy Act. Responsibilities include investigating  
18 complaints as they come up, and we're working on our  
19 process, and managing the privacy incident program  
20 through collaboration with the Enterprise Operations  
21 Center, Chief Information Officer, and security and  
22 management.

1           In addition to that, I conduct staff  
2 assistance visits to the components and I'm looking at  
3 both incidents, what's going well, what isn't, how are  
4 you safeguarding personal information, because the two  
5 -- if we can find out there's a trend, we can develop  
6 training so we can prevent incidents from occurring and  
7 also complaints, so the two are hand in hand. It's a  
8 nice collaboration there.

9           Now, not part of the slides, what we've been  
10 doing since the last DPIAC meeting -- I think the last  
11 one was September 10th and I believe Mary Ellen updated  
12 you that we have had our first, the inaugural annual  
13 core management group meeting, which OMB mandates.  
14 From the show of hands at a CPO incident group camp  
15 that I participated in, I don't know that any other  
16 agencies have accomplished this. So we had a  
17 successful core management group meeting.

18           On September 2nd we published a 25-page  
19 report which talks about incident report at the  
20 Department from 2007 through June of 2009, and it's for  
21 official use only, so I unfortunately can't release it  
22 here. But it showed the trends where we're finding

1        compromises of information, if it's hackers, emails,  
2        and particular components. We showed in FEMA where  
3        their issues were versus other agencies, other  
4        components, and they got to develop -- we helped them  
5        develop training, or if there were special things  
6        occurring. At system conferences, we learned incident  
7        reporting tends to be up. We also feel that incident  
8        reporting is not a bad thing. Increased reporting just  
9        means it's increased reporting, not necessarily that  
10       they are lax. So we were pretty happy with that nice  
11       dialogue and great comments and requests came out of  
12       that.

13                In fact, in November we had our first  
14       quarterly incident meeting, and we're going to continue  
15       that. We learned there's a different experience level  
16       in the components, so they really valued -- you think  
17       you take it for granted, just because you've been doing  
18       incident management for this many years. There is a  
19       lot to be learned with the synergy. A lot of good  
20       suggestions came out of that.

21                On September 21st I developed the DHS Privacy  
22       Incident Guidance, which is an internal Privacy Office

1 guide for how to handle an incident. We have our DHS  
2 Privacy Incident Handling Guidance. The PIHG, as many  
3 of you know, is a 100-page document on our web site and  
4 gives examples of roles and responsibilities, the  
5 technical part, what information security does, how you  
6 report an incident. We also have a desktop user's  
7 guide. This was our own internal privacy guide and  
8 with specific names, who to call in the office, who do  
9 you call, what do you do if you're there on Friday and  
10 my staff and I are not in there.

11 We did this in anticipation of the work force  
12 being out with H1N1, so we're pretty proud of that. I  
13 gave a training session to the group and interacted  
14 with real examples; not just what is an incident, but  
15 the actual categories -- compromise of information,  
16 unauthorized access, which are not necessarily  
17 intuitive. So we're saying, yes, leaving a paper with  
18 Social Security numbers on a fax machine is an  
19 incident, and making everyone aware that privacy is  
20 everyone's responsibility.

21 So that went very well, and we provided that  
22 to the component privacy officers in our role to meet

1 the Secretary's goal for efficiency so that they don't  
2 have to reinvent the wheel, as something that they want  
3 to tailor for their needs. People were pretty happy  
4 with that.

5 Then, on September 23, I participated in the  
6 CIO Council Privacy Committee Chief Privacy Officers  
7 Boot Camp and gave a presentation on incident response.

8 That's our update on what we've been doing in  
9 incidents and inquiries, and we're pretty happy about  
10 it. Now to the complaints portion on the slides. We  
11 had our -- in September, just a couple months ago, we  
12 began using our newly developed electronic complaint  
13 tracking system. It's an electronic correspondence  
14 workflow. On the next slide, the next few slides,  
15 you'll see the actual templates. It's right now just  
16 for Privacy Office use. What we're doing internally is  
17 allowing us to help compile the Section 803 reporting.

18 Mary Ellen, the Chief Privacy Officer,  
19 approved the CTS privacy impact assessment on June 29  
20 and the SORN on July 21, which are on our web site.  
21 I've spoken with our compliance section and we haven't  
22 gotten any complaint, we didn't get any comments on

1 that. So that was good news.

2 Here's the actual complaint tracking system  
3 template that we developed with our contractor. This is  
4 the interim electronic correspondence work flow system,  
5 so it's already being used by the Department. So it's  
6 very user-friendly. We came up with these categories  
7 that we thought might be applicable to Privacy Office.  
8 We won't go through it, but the things we thought might  
9 apply we checked: civil rights, fusion centers; if  
10 ever we wanted to do a report to say where are our  
11 issues, and if we're finding that we're having a lot of  
12 complaints coming in regarding the program we need to  
13 take a look at that. So that's just down the road.

14 But right now we're looking at the complaint  
15 source. They're coming in through emails, faxes,  
16 letters. "Direct" means direct to me, complaints can  
17 come in.

18 We have an IQ outlook added feature when, if  
19 it comes in by an email, I can add it in directly into  
20 this system. So this is really increasing our  
21 efficiency and it's pretty effective.

22 Since September when we started it, we've had

1 five complaints come in. We were able to track them  
2 easily. The reporting categories are straight from the  
3 Section 803 reporting, processes and procedure,  
4 redress, operational. We created this fourth one,  
5 "Referred internally to DHS component." We're finding  
6 that it's coming to us, but it would be better handled  
7 at another -- at a component level. They'll  
8 investigate and handle it, and then we would have, if  
9 the individual is not happy, our redress part of it  
10 would be investigated. So that has gone well.

11 Then another, complaint disposition. The  
12 dropdown we came up with. It gives complaint  
13 disposition and those are the three basic categories,  
14 straight from Section 803 reporting. There are  
15 complaint categories, process and procedures, some  
16 examples of that; the issues concerning appropriate  
17 access, operational, when the individual feels that  
18 privacy has been violated or sees boxes of records, so  
19 these things are things to know about. And if we're  
20 made aware of this, we can also prevent incidents. So  
21 it is nice -- the two do go hand in hand.

22 This is the disposition of complaints, pretty

1 self-explanatory.

2           Then going into -- that's the end of our  
3 complaints portion. Then the electronic complaints  
4 tracking right now is simply just tracking. I can  
5 answer your questions at the end, but that's our simple  
6 tracking system. It's only the Privacy Office, as  
7 mentioned, and we're going to see how it works out and  
8 then see if this is something we can do Department-wide  
9 to send over complaints internally. But we just  
10 started this, as I mentioned, in September and we're  
11 working out some things still. So we're pleased with  
12 that, able to get that up and operational.

13           Then the DHS Traveler Redress Inquiry Program  
14 is also part of our redress. I know you're interested  
15 in redress. Jim Kennedy, the program manager, spoke to  
16 you I believe in February about TRIP. As you know,  
17 it's a processing point for redress inquiries, for  
18 individuals seeking -- having problems with their  
19 traveling , through the secondary screening, or delayed  
20 entry.

21           The benefits are: one-stop portal, creates a  
22 channel for collaboration among redress officials, and

1 it puts the burden on the government, which is great  
2 because the public does not necessarily know what the  
3 issue is. So it's got its benefits.

4 Our role in this, the Privacy Office role,  
5 the Chief Privacy Officer participates on the TRIP  
6 Governance Board. I participate in the headquarters  
7 component working group, Office of Appeals and Redress.  
8 This is a working group where we've been actively  
9 working on the IG recommendations and how to improve  
10 the process. Our actual case management as far as the  
11 Privacy Office's role in handling TRIP cases, we have  
12 two analysts who are serving as case reviewers, and I  
13 look at the ones that are actually where privacy is the  
14 lead or that's the only issue. If we're one of many on  
15 a case where an individual believes many issues have  
16 happened in addition to privacy, the analysts in my  
17 office look at that.

18 Since January until November 18th, they've  
19 looked at 2,338 complaints where the individuals  
20 checked the block, my personal information has been  
21 misused. Of those, zero were privacy issues. So we're  
22 working with TRIP to come up with a meaningful

1 category. Normally they're secondary screening issues  
2 or issues where they thought they had been treated  
3 improperly, their documents were taken. So we're  
4 working with TRIP to learn what the actual process is,  
5 because a lot of the documents are requested for  
6 access, so they're appropriately reviewed. Or the  
7 laptop issue, looking at personal information, but that  
8 was a lot of complaints to look at and zero were  
9 privacy-related.

10 Then we also provided some recommendations on  
11 what are true privacy issues.

12 On August 13, Mary Ellen and her staff went  
13 to the TRIP program office again to learn more about  
14 what exactly they're doing, the things forthcoming, and  
15 how we can have a better role in helping them.

16 On October 13th, the IG released its final  
17 report, which I know you've had a chance to see -- the  
18 redacted version is on the web site -- of their review  
19 of the TRIP program. They had some praise for the TRIP  
20 program. It is centralizing intake of redress, it  
21 provides multiple agency case review and coordination,  
22 and it fosters information-sharing and communication

1 among the redress officials.

2 On October 22nd, I met with the Homeland  
3 Security professional Committee staff and TSA and also  
4 the Office of Policy, specifically the Screening  
5 Coordination Office, and we briefed the committee on  
6 the status of recommendations. 21 of them are still  
7 open and 5 of them have a root cause which can be  
8 addressed pretty soon. The five that have a common  
9 solution are supporting the implementation of Secure  
10 Flight, updating the response letter to improve  
11 transparency and customer focus, the TRIP template  
12 letter, and developing and acquiring second generation  
13 case management system to enhance the reporting,  
14 management, and quality control mechanisms.

15 The redress charter that I've been actively  
16 involved with is addressing the roles and  
17 responsibilities of all the stakeholders; and the final  
18 one, addressing the redress standard operating  
19 procedures for redress procedures.

20 So these five solutions will address pretty  
21 much the 21, so the IG is pretty happy with what's  
22 going on there. The committee requested an additional

1 briefing following the release of the 90-day letter,  
2 which just went out November 22.

3 We fully support what TRIP is doing and we're  
4 happy to be a part of helping them improve their  
5 process. In fact, yesterday we were part of the latest  
6 iteration of their case management system. They're  
7 updating it, and they sat down with us and looked at  
8 our SOP and asked, what would make it better. We  
9 specifically worked on recommendation number 2.

10 Then number 20 I've been involved with, but  
11 we're also looking at the other recommendations. A  
12 customer survey apparently was one of the complaints,  
13 the number 23 recommendation, that they're not keeping  
14 track of it. So they sent it to us to take a look at  
15 and ask the requester, is this useful, are you  
16 satisfied, do you feel like you've been hurt? So  
17 they're really taking the IG's recommendations  
18 seriously and implementing them and including us in the  
19 process.

20 That concludes my presentation.

21 CHAIRMAN PURCELL: Thank you, Rose.

22 My cluster analysis shows that this corner is

1 particularly concerned. So we'll start with David.

2 Mr. Hoffman.

3 MR. HOFFMAN: First, thank you very much for  
4 coming. This is fascinating, to see how much work is  
5 going on, plus to see the tremendous volume that you're  
6 faced with. It's got to be an incredible challenge.  
7 But this is absolutely great work.

8 I just wanted to clear up a couple things  
9 that I think maybe I'm the only one who's confused on.  
10 In the TRIP portion of the discussion it says, speaking  
11 to the volume, that the DHS Privacy Office reviewed  
12 2,378 complaints that come through TRIP. Then on the  
13 complaint tracking system, in the template as one of  
14 the input mechanisms it has the complaint source is  
15 TRIP database. But then I heard you say that there's  
16 only five since September.

17 So I was trying to figure out. Are you guys  
18 at least at this point thinking of the complaint  
19 tracking system as an escalation out of those 2378?

20 MS. BIRD: That's actually separate. When  
21 this was created, it allowed for the possibility that  
22 we might need to -- a complaint moves over to the TRIP

1 system. So we included every field. So they're  
2 separate right now. TRIP has its own PIA, its own  
3 SORN, and its own system. As I said, right now those  
4 2,378 complaints we get through the TRIP database where  
5 a person has checked "secondary screening issues" and  
6 "my personal information."

7 So we're reviewing it under TRIP. But the  
8 idea, if there were a real privacy issue that we needed  
9 to investigate, go in and investigate, it would likely  
10 come out of -- we would move it over to here and check  
11 the TRIP database and put the TRIP case number. Not  
12 that we haven't -- we haven't acted on this yet. It's  
13 still -- we just included that field for the  
14 possibility, but yes, they are separate right now.

15 MR. HOFFMAN: So the intent of the complaint  
16 tracking system, am I correct in interpreting that this  
17 is really a system to make sure where there are ad hoc  
18 complaints that are made that aren't captured in an  
19 already existing system like TRIP, you guys wanted to  
20 have a place to congregate those, assess them, and be  
21 able to handle those? And this is almost functioning  
22 as a test right now to see if that would be expanded?

1           Because I took from what you're saying, right  
2           now it's only the complaints that are coming in to the  
3           Privacy Office directly; it wouldn't be something that  
4           comes into a component and then gets referred as a  
5           question to the Privacy Office? I'm just trying to  
6           figure out what the input mechanism is.

7           MS. BIRD: It's any complaint. So if  
8           something came -- let's say ICE investigated something  
9           and the individual was not happy or wanted us to review  
10          it. We would put it in our complaint system. It would  
11          get logged in as a complaint from ICE.

12          MR. HOFFMAN: Okay.

13          MS. BIRD: Right now it is a tracking system  
14          for anything and it could come in in any mechanism.  
15          Just TRIP is its own system. When this was created we  
16          wanted to include every field since it's just a --  
17          since we were just beginning it.

18          MR. HOFFMAN: I'll beg the Chair's  
19          forgiveness and ask one more question. So it seems to  
20          me a little bit of a mismatch to have over 2300  
21          complaints coming in to TRIP, but only 5 since  
22          September into this system. I'm wondering if you

1 conclude from that that there's a possibility that  
2 there's a need to go out and do some awareness about  
3 the need to have people bring complaints in to  
4 categorize them?

5 It just seems that number five seems  
6 interestingly low.

7 MS. BIRD: Well, five is just what we've  
8 gotten through the email, through the: I believe my  
9 medical information was misused, I believe I'm being --  
10 one example: I believe I'm being harassed basically  
11 because my medical records were provided to somebody  
12 that did not have a need to know. So that's a true  
13 complaint.

14 And as far as the tracking, I asked the  
15 question too when I had to provide our figures for the  
16 Section 803 reporting that was just due. The way that  
17 the TRIP complaints count is where privacy is the lead.

18 So privacy is the lead where they thought privacy was  
19 the only issue. So for this, this is not listed in  
20 this complaint source, but there were seven. So from  
21 September to November 30th there were seven TRIP cases  
22 where privacy was the only issue, the person thought

1 his personal information had been checked.

2 MR. HOFFMAN: Okay.

3 MS. BIRD: Am I confusing you?

4 MR. HOFFMAN: No, you're not confusing me. I  
5 think just the last comment to me would be that number  
6 I think as we've been looking at redress, a couple  
7 things we've been looking at as elements of redress  
8 would be accessibility and availability. Just you know  
9 the data a lot better than I do, but my initial  
10 indication when I would see only five folks coming in,  
11 it would lead me to want to raise the question to say,  
12 is this as accessible and available? We really think  
13 that there's only five complaints that should have come  
14 in during that period of time?

15 It may be that really that is the right  
16 amount.

17 MS. BIRD: Right. As Mary Ellen mentioned,  
18 we just hired a communications director, so I am  
19 working with him, and that might be a place on the web  
20 site, complaints. Since we just began our system, I  
21 was thinking that too, an outreach. He is working on  
22 updating the web site, as Mary Ellen mentioned. Right

1 now it's not something we're necessarily excited about.

2 But as we go forward, that is a way.

3 But TRIP is definitely a separate system.

4 MR. HOFFMAN: I'd like to commend the hard  
5 work that it takes to put the other system in place.  
6 And it is just recently, so I'm not saying that as a  
7 criticism.

8 MS. BIRD: Oh, no, no.

9 MR. HOFFMAN: It just seems like an  
10 opportunity, actually.

11 Thank you, Mr. Chairman.

12 CHAIRMAN PURCELL: Thanks, David.

13 Ramon.

14 MR. BARQUIN: Rose, I will echo about 100  
15 percent of what David said, and this point. There's  
16 two parts here that I would like to understand. There  
17 are a lot of components throughout the Department that  
18 I'm assuming also get complaints and in many cases  
19 require redress. I'm sure the Coast Guard's  
20 occasionally got a complaint about, you saved my life,  
21 but you sunk my boat, whatever.

22 The question is, insofar as there are privacy

1 components in a lot of these complaints is there or  
2 should -- your system may start to become a Department-  
3 wide repository for handling these.

4 The second one is, I would like to take the  
5 position here at least to say that no complaint, no  
6 complaint, should ever have no action required. I  
7 mean, I was sort of looking at your -- even if it's a  
8 response that said, thank you, Mr. or Ms. Citizen, and  
9 here is a response to your complaint. At the very  
10 least, some type of a response.

11 I saw your example that says a complaint  
12 regarding a published PIA or final rule, and I would  
13 think that that one in particular, for privacy, should  
14 be a response: We think that this is correct because.  
15 Just I wanted to actually state that position, that any  
16 complaint should have some type of action.

17 MS. BIRD: That example was given, I believe  
18 somebody, they're just unhappy with the way something  
19 was written. That was my understanding. So there was  
20 no action required if they complain and are unhappy --  
21 more like not a complaint seeking redress: I don't  
22 like that you collect personal information, I don't

1 like Secure Flight, I don't like that I have to give my  
2 gender. So there might not be any action required.  
3 You're just unhappy with or expressing a  
4 dissatisfaction.

5 But also, the no action required, one of the  
6 ones we did have was it's a duplicate. We were cc'ed  
7 to another component, the actual component. So it  
8 could be no action required because it's a duplicate.

9 MR. BARQUIN: When it says no action  
10 required, is there no response? It's sort of like,  
11 here I am a citizen, a taxpayer, I send in a complaint  
12 and it falls into the black hole. That's where I was  
13 coming from. I don't mean let's change the PIA and  
14 let's change the rule.

15 MS. BIRD: Oh, no. There's a response.  
16 There is a response back, like in an email: This has  
17 been properly handled by this component. We see you  
18 sent this as a courtesy copy to us. So we send a  
19 response, but there was no action.

20 CHAIRMAN PURCELL: There's no root cause  
21 analysis that's required.

22 MS. BIRD: Right.

1 Yes, the second 803 categories, we didn't --

2 MS. RICHARDS: Can I just clarify on one of  
3 those in particular. Some of the complaints that are  
4 counted -- I'm sorry. I'm Becky Richards, Privacy  
5 Compliance Director.

6 Some of the complaints that don't go through  
7 hers, but are the comments that we receive on the  
8 SORNs, the NPRMs, and the final rules associated with  
9 the Privacy Act system of record notices. So it was  
10 determined when we were going through 803 reporting  
11 inter-agency that those would be counted sort of as,  
12 quote, "complaints" under this. So some of those  
13 numbers, you're not going to send an email back, but we  
14 may respond back by publishing the PIA or publishing an  
15 updated final rule that addressed those comments.

16 I realize that's a little confusing. That's  
17 sort of the background of why there's ones, like where  
18 it says it's on a PIA or an NPRM. There's no response  
19 or there may not be a response taken.

20 MR. BARQUIN: I'm sure the dictionary  
21 differentiates between a comment and a complaint. If  
22 you're required by law to do something, I think we just

1 need to find a way to at some point modify it.

2 CHAIRMAN PURCELL: And one can always take  
3 steps that aren't required by law, but are just the  
4 common courtesy of responding to an inquiry.

5 I have next Kirk.

6 MR. HERATH: Thank you.

7 I may be one of the people here who's  
8 actually excited by this presentation, because this  
9 probably is the most important element of the Privacy  
10 Office. When I met you last fall, I think I told you  
11 that this is a tough job. I'm 5 years into this and I  
12 can tell you that where we were 5 years ago and where  
13 we are today is just completely different. You have  
14 evolved, you learned.

15 I do have a couple questions here. So the  
16 composition of your team, obviously -- is there any way  
17 that we can get sort of your manual on how you do this?

18 MS. BIRD: What specifically?

19 MR. HERATH: Everything. Just I would be  
20 interested in looking at it.

21 MS. CALLAHAN: Complaints or incident  
22 handling?

1           MR. HERATH: Incident handling.

2           MS. CALLAHAN: Oh, sure.

3           MR. HERATH: I assume you have more of a  
4 federated team, right?

5           MS. BIRD: Yes.

6           MR. HERATH: Typically do you have -- is  
7 there a typical composition that you find, and who  
8 handles that? So these things tend to be -- you have  
9 to have somebody who manages each of these  
10 investigations?

11          MS. BIRD: For privacy incidents?

12          MR. HERATH: For privacy incidents, where  
13 somebody has mailed somebody the wrong information.

14          MS. BIRD: A team gets involved and,  
15 depending on how it happens, the person reports it to  
16 the program manager in the component. The program  
17 manager reports it to the information system security  
18 officer, who then -- we have a template where, just  
19 like this, they type in the information, as much  
20 information as possible. It was an email, it was  
21 unencrypted, it had five socials.

22          So it gets sent to the Enterprise Operations

1 Center. They take a look at it and give it a  
2 significant or a minor code. This whole process goes  
3 on behind the scenes. The Enterprise Operations Center  
4 sets up, I guess it's a case number, and we get  
5 automatic alerts depending on the level.

6 Mary Ellen has included in the IG this whole  
7 group with the summary. That's behind the scenes.  
8 It's almost like in the Army. The IT team is working.  
9 The privacy part of it in the component is ensuring  
10 privacy training is in place, that, okay, if you sent  
11 an email or whatever the issue was, we require that  
12 they take a culture of privacy training or have shown  
13 that they've learned what the issue was and it won't  
14 happen again.

15 Then they send an email or they type,  
16 depending on -- we've given the components, the ISMs,  
17 the information security managers, or officers, or the  
18 privacy point of contact, type into the template:  
19 Individual has been counseled and training has been  
20 administered. That way it's on the record that they've  
21 learned and it likely won't happen again.

22 MR. HERATH: So is there a root cause

1 analysis done, and who does it? Is it the information  
2 security, the CIO? Is it you? So there could be a  
3 lack of training is the root cause and that's fine.  
4 But it could also be system integrity. It could be  
5 application error. It could just be a process that is  
6 somehow wrong, and so you've got to -- it's almost like  
7 -- this is why this is such an essential element from  
8 an integrity perspective, because it is literally a  
9 learning loop.

10 The way I think I explained this to you last  
11 fall is, you'll see it's like lifting up rocks and  
12 finding things underneath them, right? They're there.  
13 But I always get a kick out of the fact that people  
14 say, oh, we've never had any breaches. That's like,  
15 oh, we're a really stupid organization, because you'll  
16 see your incidents climb like this (indicating) over  
17 years, but then you'll see your impacts go like this  
18 (indicating).

19 If you do it well, if your metrics are good,  
20 you'll have this wonderful arc up of incidents and  
21 investigations and this incredible arc down of actual  
22 impacted, in fact we call them, affected individuals,

1 people whose stuff was improperly accessed, authorized.

2 So if you don't have a metric around root  
3 cause, every one of these should have a root cause  
4 analysis in your metrics, I would suggest, and then you  
5 should have a metric of how many root causes have been  
6 completed and closed. Now, it could be you just kick  
7 these over to the information security guys and they do  
8 it for the business or in this case the agency or the  
9 government. Somebody's got to be accountable. They  
10 are almost little mini-assessments, is really what  
11 results from this.

12 MS. BIRD: I believe this is going on. I'll  
13 check with the information security managers. This is  
14 going on at their level.

15 MS. CALLAHAN: It is going on. But I agree  
16 with you that we have to --

17 MR. HERATH: It would be good for you to  
18 track what they're doing so that you can keep them,  
19 hold them accountable, to make sure, because you'll  
20 find that the better a root cause analysis is done and  
21 the more of them are closed, your impacts down the road  
22 become less and less and less. The system actually

1 gets smarter. It learns. You learn from your mistakes  
2 and you constantly are refining your processes and your  
3 applications and your system, and you're driving to  
4 ultimately zero defects. You never get there, but you  
5 get pretty darn close.

6 MS. BIRD: That's what we're trying to do  
7 with our incident quarterly meetings. Like some of our  
8 components don't experience things the way somebody  
9 else does, but if we can say --

10 MR. HERATH: I think, going back to what was  
11 stated here, I think the fact -- I think that you need  
12 Department-wide, at least, you need to track all of  
13 this in one place. I would encourage you not to have a  
14 balkanized incident --

15 MS. CALLAHAN: It is all tracked at the  
16 operations level.

17 MR. HERATH: It is?

18 MS. CALLAHAN: Yes. That's where the root  
19 cause analysis is taking place and so on. But I agree  
20 with you that we should be hooked in. With regard to  
21 the numbers, Rose can talk to you, but they have  
22 increased and the impacts have decreased, absolutely.

1           But I appreciate your comments about having  
2    privacy and the operations people work together more  
3    closely.

4           MS. BIRD: That is a great idea, because we  
5    can't have them anonymizing information to provide.  
6    That's what we're trying to do for the privacy part of  
7    this, is seeing what's going on, and what we're seeing  
8    is increases in email sending to somebody who has a  
9    similar name. It's a need to know, yes, but it's the  
10   person with the same name. It's happening.

11          MR. HERATH: You're right, it happens all the  
12   time. So the "no action required," that's interesting.  
13   I figured they were sending something out. So who  
14   makes the determination for "no action required" Is it  
15   a legal analysis, a legal opinion that's issued around  
16   this? Or is this administrative?

17          MS. BIRD: Right now it's administrative.  
18   We're going to be putting a process in place, looking  
19   at our complaints management, what would be the best  
20   process. But I'm reading it and determining, since I'm  
21   in the complaints role there, seeing who would likely  
22   handle this, and does this make sense.

1           The ones that have come in have clearly gone  
2     in a component issue. So the analysis in reading is  
3     this. I did have one prior to our complaint tracking  
4     system in place, an individual had a complaint about  
5     her medical records. She had a complaint about an  
6     office. Her medical records were not there, so she  
7     wanted me to look into it. So I sent a note in  
8     response in my role as director, investigated her  
9     complaint. It was logged as an official complaint.  
10    She gave me the point of contact and I sent an email to  
11    the person.

12           So it didn't rise to the level of needing to  
13    be legal because there was an extensive email trail  
14    that showed she had been told to go get her medical  
15    records from this office, they hadn't lost them, she  
16    had to come in, and then she had to provide them to the  
17    Department of Labor. So action was required on her  
18    part. So that was a quick -- legal didn't need to be  
19    involved.

20           But if it had risen to a level where the  
21    medical records were lost, it would then go to the next  
22    step. But luckily, it proved the person had done her

1 due diligence, many emails saying: Come in to the  
2 office, I'm here, they're right here; you haven't lost  
3 your records.

4 MR. HERATH: Okay. But there isn't a legal  
5 opinion done very often around whether something is or  
6 is not legally an unauthorized access? Is the OGC  
7 reviewing these, these incidents, on a regular basis, I  
8 guess?

9 MS. BIRD: Well, they haven't had any regular  
10 --

11 MS. CALLAHAN: When we've needed to, we have.  
12 General Counsel has been intimately involved on some of  
13 those more complicated questions.

14 CHAIRMAN PURCELL: Kirk, I'm going to cut  
15 this because we do have other questions. But I do want  
16 to emphasize that we always hear that privacy is a cost  
17 center and there's no benefits to it, but one of the  
18 ways you can demonstrate benefits from this kind of a  
19 program is to close this loop and start demonstrating  
20 that, in addition to the benefits and costs of this  
21 tracking and mitigation effort, that there are specific  
22 benefits that accrue as well. And that's a good report

1 card, and you've got aces for actually generating those  
2 kinds of reports.

3 Joe.

4 MR. ALHADEFF: Thanks.

5 I'll join the others and say I think the  
6 progress that's been done is a very welcome  
7 development, and the screens are actually pretty  
8 impressive. I'm going to look at two specific issues  
9 and follow-ons on the topics that have been raised.

10 To Kirk's point about the centralized need to  
11 maintain this, one of the reasons is because too often  
12 you look at a root cause that's been closed and you  
13 figure that's done. What you may find is if you  
14 analyze across root causes, what you find out is it's  
15 not a failure of the system or a failure of the person;  
16 it's the failure of a policy, process, or what have  
17 you. So the root cause at the aggregate level helps  
18 you see if there are too many incidents, then maybe you  
19 need to look somewhere else besides what the root cause  
20 that was identified was, because it might be something  
21 else. So that centralization is very useful in making  
22 you a learning organization.

1           The other question goes to David's point,  
2     that David may have gotten clarified, but I'm still  
3     stuck on. There were 2,000-plus complaints that the  
4     person who was complaining thought that there might  
5     have been some aspect of a privacy issue, but none was  
6     found. I guess my question is, did that lead you to  
7     think that perhaps going back to the definition of a  
8     privacy incident may be useful? Because if someone is  
9     perceiving that their privacy is at risk, then perhaps  
10    there is a -- in a legalistic definition, was  
11    information wrongfully used, the answer is no and there  
12    was no chance of that happening. But there was a  
13    perception that it was happening or could have  
14    happened, and that perception needs to be addressed.  
15    Otherwise the dissatisfaction of people in that  
16    situation will continue.

17           MS. BIRD: That is an education. That's the  
18    form on the TRIP screen that says "I believe my  
19    personal information has been misused." So we're  
20    trying to work with them to work with them as they  
21    update their system, what would be a meaningful  
22    category, because the person believes his information

1 has been misused. Some of the examples: I was moved  
2 to secondary screening; I'm always asked my name. So  
3 that's not a true privacy, like your personal  
4 information. He perceives it to have been misused.

5 Also, his identity was stolen. So yes, his  
6 information was misused, so he's saying: My identity  
7 was stolen; every time I go through, I get sent to  
8 secondary screening. So for that particular, the  
9 reason for that complaint, that issue that the privacy  
10 office saw, we feel it's because of that category, and  
11 we're trying to work with them on how to make it  
12 meaningful and give an example of what is a true  
13 privacy issue.

14 MR. ALHADEFF: Well, but the other aspect  
15 might be to respond to the privacy aspect of the  
16 concern, and the explanation of why there wasn't misuse  
17 is kind of an important way to build that education.  
18 So what I'm saying is it's an incident that is not --  
19 to use the words that have confused everybody, it's an  
20 incident that may not require an action, but does  
21 require a response, because there was no privacy  
22 violation, but you certainly need to explain why there

1 wasn't.

2           Then that starts -- unfortunately, that's the  
3 one by one which sucks, to use the technical term,  
4 because there's just no bandwidth for doing it that  
5 way.

6           MS. BIRD: Well, you're making a good point,  
7 because when we met with the case manager that's part  
8 of what we needed to know to give a meaningful  
9 category, was what are the processes at TSA, at the  
10 airport what is required, what documents are collected.  
11 So that what you're saying is not a misuse because by  
12 definition to get on the airplane you have to give your  
13 personal information.

14           MR. ALHADEFF: But explaining why that isn't  
15 and explaining -- if something keeps on hitting  
16 secondary screening, it's something they're going to  
17 figure out.

18           But I know Richard's got time constraints, so  
19 I'll leave it at that.

20           CHAIRMAN PURCELL: We do. But I think that,  
21 just to use a little bit of the time for my  
22 prerogative, I think that what the Committee is trying

1 to get to here is not just the legalistic, gosh, this  
2 either fits the category, the defined government view  
3 of a category of use or misuse of the data, but  
4 citizens of the United States are still feeling like  
5 victims of that same process, and explaining how that  
6 process is designed to protect citizens and not  
7 victimize them may go a long ways toward educating the  
8 public.

9           And you're in a particularly useful position  
10 to do that. Secondly, if a person keeps hitting  
11 secondary screening, there is an indication that  
12 perhaps there is something endemic there either in the  
13 person or in the system and it does beg for a little  
14 further review perhaps, even if legalistically and  
15 according to a very cut and dried analysis it can be  
16 dismissed as a "no action required." There may be an  
17 analysis that puts that kind of thing in a parking lot  
18 that begins to beg more action because you really have  
19 perception issues. Perhaps your communication person  
20 needs to take that up. Perhaps Mary Ellen needs to be  
21 fully informed of those kinds of things. And postcards  
22 and emails do go a long way to making people feel like,

1 fine, I've been heard.

2 If people aren't heard, they will complain  
3 again and again and again, and your system will begin  
4 to not learn very well because you get repetitive kinds  
5 of things that are not necessarily of value. But it's  
6 not that person's problem; it's perhaps the problem of  
7 the response itself.

8 Now, we do have quite a few people, so I'm  
9 going to take two more questions. They're going to  
10 have to be quick. And I do encourage follow-ups in  
11 writing. So pass me your follow-ups. We'll make sure  
12 that Ms. Bird gets those and we get a full response to  
13 those.

14 So we've just lost all but two. So I guess,  
15 let me see. Who had -- Lisa, you were up first.

16 MS. SOTTO: I'll be quick.

17 You wear two very distinct functions and  
18 important functions. Turning to the breach function,  
19 we know that incidents occur both as a result of  
20 systems and employee actions internally and of course  
21 always as a result of service providers' actions. So  
22 I'm wondering, on the contractor side, it's easier --

1 you have a very difficult workforce to work with, going  
2 from the workforce internally, very hard to control  
3 contractors' use of data and compromises.

4 So I'm wondering what the percentages are of  
5 the internal versus external data compromises? And I  
6 don't mean external to your system; I mean data  
7 compromises at the contractor level versus at the DHS  
8 level. So the percentages there.

9 And then what you're doing to manage incident  
10 issues at the contractor level?

11 MS. BIRD: Well, we haven't been tracking  
12 whether it was a contractor that used our system and  
13 violated it. We haven't been tracking that. But we  
14 consider -- actually, I met with GAO just recently on  
15 this issue of looking at contractor access to sensitive  
16 data. So the contractors when they come on board,  
17 they're vetted and they sign a nondisclosure agreement.  
18 They agree to participate in programs that follow our  
19 standards.

20 MS. SOTTO: I'm actually thinking about  
21 contractors who are organizations who work with, who  
22 have data, who develop data externally and work with

1 the use of it. They have laptops with data, that sort  
2 of thing. Not the contractors who are working on  
3 individual systems.

4 MS. BIRD: I could get back to you. I  
5 haven't really followed that. We haven't tracked that.

6 MS. CALLAHAN: I'll talk to you about that.

7 CHAIRMAN PURCELL: So contracted service  
8 providers who may present an external vulnerability.

9 MS. SOTTO: People who have a laptop because  
10 they're performing a function for DHS, and their  
11 laptops can be stolen.

12 CHAIRMAN PURCELL: Right, right. And how  
13 that's reported up. Good, cool. That's a good follow-  
14 up area.

15 Lance, take us to the break, please, quickly.

16 MR. LANCE HOFFMAN: You want to break? I'll  
17 do it quickly.

18 CHAIRMAN PURCELL: Thank you.

19 MR. LANCE HOFFMAN: Again, thank you. We've  
20 certainly come a long way, as Kirk says, since the  
21 early days. We've made a lot of progress in that  
22 regard.

1           I wonder if this is more than a complaint  
2 tracking system. I wonder if that's the best  
3 description of it. It seems maybe you could add some  
4 other things. I'm not sure.

5           But more importantly, as per Ramon's comment,  
6 it says it's the Privacy Office complaint tracking  
7 system. Yet it talks to other systems. I'm still a  
8 little bit confused about why that is and what the  
9 rationale is. I understand maybe to get things going  
10 you have to do it that way, but it seems like this  
11 could be done right, a model. There could be a  
12 Department-wide system, either federated or non-  
13 federated, and maybe you're looking at that or could  
14 look into it. I was wondering if you have any response  
15 about that.

16           The other thing, it ties into a general  
17 comment which came out in the redress group yesterday.  
18 This is an opportunity to think strategically and not  
19 legalistically. I want to echo what legal counsel  
20 said. I think there are a number of people who may be  
21 under the impression that DHS really is going through  
22 legal stuff, and that's fine. But you may be missing

1 the forest for the trees. It's working at that.

2 But what I'd like to see also, which I don't  
3 see here, but maybe the privacy complaints are too  
4 small, examples of the reports. Mary Ellen said that  
5 at a Department level or a system level they look at  
6 things. I don't see it here. Maybe it's just because  
7 --

8 MS. CALLAHAN: That was for breaches. Sorry  
9 if I wasn't clear. The breaches are there, and the  
10 complaints are inbound complaints.

11 MR. LANCE HOFFMAN: Okay. But I'm thinking a  
12 general tracking system, you should be able to mine it,  
13 I would think. It's an opportunity not to be missed,  
14 rather than just, okay, we had to do complaint tracking  
15 because we weren't doing it, so we'll do it. And  
16 I'll stop there, because I think it's something a lot  
17 of other people were saying.

18 CHAIRMAN PURCELL: Great. Thank you.

19 I think that the summation I would provide is  
20 that the complaint handling system is way ahead, as  
21 people have said, from what we've seen and experienced  
22 on the committee. Certainly citizens of the United

1 States have waited 5 years during this process, too,  
2 and they continue to wait for improvements. And I'm  
3 sure that these improvements will be available soon.

4 At the same time, I think one of the things  
5 the committee is saying is an incident handling process  
6 that protects the Department's exposure to  
7 vulnerabilities is necessary, but also there's an  
8 inquiry handling process that is more like a customer  
9 service process that we believe is also valid and  
10 necessary, and we don't want to see the protective  
11 nature of an incident handling process take precedence  
12 entirely and eliminate the customer service side. The  
13 customer service side is also quite important, we  
14 believe.

15 Just because it's not an illegal act doesn't  
16 mean somebody's privacy hasn't been violated in their  
17 own personal terms, and they may need some reassurance  
18 that the Department is not evil. We would like to see  
19 that reassurance being put forward on a regular basis  
20 and vociferously.

21 We think that this is a great progress.  
22 Don't mistake our comments for anything else.

1           Ms. Bird, thank you very much. We appreciate  
2 your time today.

3           MS. BIRD: Thank you.

4           CHAIRMAN PURCELL: We'd like to take a short  
5 break at this time. Please remember that we are -- at  
6 15 minutes, we'll begin at -- well, let's make it at  
7 10:20 and we'll be okay. We'll start at 10:20 whether  
8 you're here or not. So if you're here, you'll hear us.  
9 If you're not, you'll disturb us by coming in late, so  
10 don't do that, please.

11           Again, if you wish to address the committee,  
12 please sign in at the table on the outside, and we'll  
13 take those comments at 11:45. Thank you.

14           (Recess from 10:08 p.m. to 10:18 p.m.)

15           CHAIRMAN PURCELL: Again, cell phones that  
16 are not silenced will be. Again, if you would like to  
17 address the committee later at the close of our  
18 session, prior to the close of our session, there is a  
19 sign-up sheet outside. We do require that you indicate  
20 your interest in addressing the committee through that  
21 sign-up sheet.

22           I'd like now to introduce our next speaker,

1 Ms. Patricia Cogswell. Patricia, welcome. She is the  
2 Acting DHS Deputy Assistant Secretary for Screening  
3 Coordination. Her portfolio in the Screening  
4 Coordination Office includes setting policy and  
5 direction in order to harmonize the many -- and we do  
6 emphasize, "many" -- DHS screening programs.

7           These programs include many of the  
8 immigration reform efforts, those involving screening  
9 to identify known or suspected terrorists, and the  
10 integration of biometric technologies and capabilities  
11 into those screening systems.

12           Prior to joining the Screening Coordination  
13 Office, Ms. Cogswell served as the chief strategist for  
14 DHS in the U.S. VISIT program and as the Director of  
15 Immigration Services Modernization for U.S. Citizenship  
16 and Immigration Services. So with a healthy resume of  
17 components work, Ms. Cogswell, welcome. You may  
18 proceed.

19           DHS SCREENING COORDINATION OFFICE UPDATE  
20           BY PATRICIA COGSWELL, ACTING DEPUTY ASSISTANT  
21           SECRETARY FOR POLICY, SCREENING COORDINATION, DHS

22           MS. COGSWELL: Thank you very much. I'm very

1 glad to be here. This is actually my second time  
2 before this committee. I spoke on actually, I believe,  
3 U.S. VISIT a couple years ago, actually at least more  
4 than three. So great to see a number of you again.

5 I believe also my predecessor Kathy Kraninger  
6 also came and addressed the committee, I'm thinking  
7 about 2 years ago. So some of this you may recognize  
8 and remember from that, but hopefully some of it will  
9 be refreshing and new.

10 So with that said, we wanted to do just a  
11 quick help set the stage for why is there a Screening  
12 Coordination Office, what is screening generally, what  
13 are some of the strategic efforts and initiatives that  
14 we're trying to undertake in this arena, and then focus  
15 more specifically into some of the program areas of how  
16 are we moving into these efforts.

17 So once upon a time prior to 9/11 and soon  
18 after 9/11, the Department of Homeland Security pulled  
19 together about 22 different agencies, as you well know.  
20 Both before that and after that, there were significant  
21 efforts to increase the number of screening activities,  
22 how they were done. As you all well know, the answer

1 was those were all done at different times, under  
2 different authorizations, with different management,  
3 and therefore they were wide-ranging and did not share  
4 any kind of common policy, common strategy. But they  
5 were all very important to move forward as fast as  
6 possible.

7           Soon after the creation of Homeland Security,  
8 it was pretty widely recognized that, gosh, you know,  
9 this was critical work that we need to do, but really  
10 we need to be smarter. We need to find a way to get  
11 more bang for our buck, to think things through, to  
12 have consistent answers between components or within a  
13 component between different programs. That's some of  
14 the things we're doing.

15           As part of that, and coming out of the 9/11  
16 Commission report and a number of these other areas,  
17 the administration said: We need to create a Screening  
18 Coordination Office whose job is to try to harmonize  
19 what's going on at least in DHS. With that said, it  
20 then went through a lengthy budgetary process where  
21 there was lots of back and forth of, should there be a  
22 consolidation of programs versus a coordination of

1 programs. As you can now see from our office, we ended  
2 up on the coordination aspect, not consolidation  
3 aspect, and have been doing so for about the last 3  
4 years.

5 In addition, when we were created, as you all  
6 well know, there was a very big focus on appeals and  
7 redress -- again, very similar. We get different  
8 answers from different components. Each one may be  
9 logical on its own, but when you compare them next to  
10 each other they don't make sense.

11 Everybody said this is really an important  
12 area to get right. About \$7.5 billion of the  
13 Department's budget a year, or a quarter of the  
14 Department's budget, is on screening-related  
15 activities. This is a huge area for the Department to  
16 try to say, how do we do this more smartly.

17 So with that said, we were created, and we  
18 have been serving three primary roles since creation.  
19 The first one is focusing on establishing an  
20 overarching framework around the policy development,  
21 strategy, the oversight, to say how do we want this  
22 landscape to make sense, so that these programs are not

1 duplicating each other, they're harmonized with each  
2 other, we know where one stops and the other one  
3 starts, we understand how they relate to the authority  
4 and what mission they're supposed to be coming out of.

5 We also often serve as the program advocate  
6 for a number of these programs. Obviously, being in  
7 the Office of Policy, one of our big focus points will  
8 be those programs that are designated as administration  
9 priorities. In addition, we also say there are  
10 opportunities where we can designate a specific  
11 program, a specific project, a specific entity as  
12 something that we say, that's the one that we see as  
13 needing to be DHS-wide the way to do something. As  
14 that role, it's really hard for a program to come  
15 forward or an organization to come forward and go: I'm  
16 the DHS. They need someone there to say: No, no; we  
17 have designated them, and this is what it means for  
18 them to be a DHS service.

19 The last aspect we perform is the portfolio  
20 manager. This really is looking at all the various  
21 programs, projects, as they come through with their  
22 investments to say: Are you following the direction

1     you were given? Are you complying with the strategy?  
2     Are you heading in the direction we expected you to?  
3     Those who do go through very quickly. Those who don't  
4     spend a lot more time answering questions about, why  
5     are you not in the place we were expecting you to end  
6     up?

7             So with that said, moving on to screening.  
8     Screening is the systematic examination or assessment  
9     done especially to detect a specific threat or risk or  
10    any particular substance, attribute, person, or  
11    undesirable material. That's pretty broad-ranging. So  
12    with that we try to identify subcomponents of that.

13            We think of screening as falling into two  
14    main buckets. One is information-based screening. So  
15    in the people arena, information-based screening really  
16    focuses on how are we doing on our suspected terrorist  
17    checks, how are we doing with criminal history checks.  
18    If employment authorization is required, how are we  
19    making sure you can be legally employed in the United  
20    States? If it's someone's immigration status, is that  
21    an appropriate status for the benefit or activity  
22    they're trying to perform? In the cargo world, there's

1 known shipper programs and other aspects. Physical  
2 screening is much more about things around a person, so  
3 things like metal detectors that we're used to. In the  
4 cargo world again, this would be actually equipment  
5 where you look at the containers.

6 I'd also like to say, scope of screening,  
7 where does it occur. Some of it is outside the United  
8 States before they come here, so it's at the border.  
9 Some of it's within the United States. So outside the  
10 border, the ones people think about are the Electronic  
11 System for Travel Authorization, ESTA, the visa  
12 process, or the container screening initiative. At the  
13 border, it's things like traditional entry passes, your  
14 passport inspection, U.S. VISIT process, radiation  
15 inspection, port monitors. Inside, things like when we  
16 do screening for domestic aviation, critical  
17 infrastructure workers, first responder identification  
18 credentials, and again the requirements to verify  
19 immigration status or eligibility.

20 With that said, we like to give a couple  
21 examples of how big DHS is in this regard. I just want  
22 to note that in general when I go talk to other

1 agencies it's very interesting to be able to compare  
2 size and scope. We've had to try to kind of approach  
3 this in a very different way than most other agencies  
4 do because they'll have one or two programs and they're  
5 really small, or they have one program that's pretty  
6 big, but it's one program, and they don't have to  
7 wrestle as much with the various intricacies and the  
8 fact that we have new stuff, new requirements, coming  
9 up on a regular basis and we have to say, well, let's  
10 not look at this from scratch, let's think about it in  
11 context of the other things we do. How is it like  
12 this? How is it not like this? So that what we do  
13 makes sense and is rational across the processes.

14 So with that said, we have our own situation,  
15 millions of screenings per day as part of the DHS  
16 family of activities. Obviously, the big ones people  
17 think about are processing at the ports of entry, 1.2  
18 million inbound travelers; 1.8 million domestic air  
19 travelers; 135,000 biometric checks a day; 30,000  
20 benefit applications. Recurrent vetting, which I will  
21 explain more. That's a term that not everybody knows.  
22 And that ability to do employment eligibility checks.

1           Just to briefly go on to that, recurrent  
2   vetting is a term we've developed to basically go  
3   around the idea that there are some individuals who  
4   have an ongoing relationship with the agency, right.  
5   They were granted the license, privilege, or status to  
6   do something for a period of time. During that entire  
7   time of that relationship, they're required to maintain  
8   all the eligibility associated with that. If you were  
9   vetted on day one and you didn't have any disqualifying  
10  criminal history, on year two out of year five you  
11  committed a disqualifying criminal history, you're no  
12  longer eligible for that status.

13           So we would want a way to say you can't have  
14  a status once you become ineligible for it. The way to  
15  do that from our perspective is recurrent vetting. In  
16  our mind, the best way for recurrent vetting does not  
17  mean throwing data against flash lists over and over,  
18  but to look for an environment where I am proactively  
19  notified of information that may say, this person is  
20  ineligible for the status.

21           All right. In 2006 we did our first shot at  
22  saying, we need to look at what are the core problem

1 areas in this arena and what is the strategic go-  
2 forward direction you want to set for screening and  
3 credentialing. We really focused on things like  
4 inefficient information and data collection. We often  
5 require individuals to provide the same information  
6 that's already been collected previously. The big ones  
7 where we get asked about this a lot are, for example,  
8 in the transportation arena, where the same individual  
9 who just got cleared for a hazardous material  
10 endorsement is asked to start over again and submit the  
11 same information to TSA for a transportation worker  
12 identification badge, and of course is charged a fee  
13 again to complete the same screening he just completed.

14 I can't tell you how often we hear from that  
15 community about how they would like to not do that.  
16 Obviously, it's in our interest and in their interest  
17 to be able to say: You've seen me before; please re-  
18 use my prior screening to expedite my process for this  
19 new benefit that I've asked for; don't start over when  
20 you, TSA, have already seen me.

21 Another one is local credential issues. When  
22 I first started in this job there was an awful lot of

1 people who thought, we really should have just one  
2 card, there should be one card. I will tell you that  
3 from day one I was never a one-card person. My belief  
4 is 157 cards is not the right answer, but one really  
5 isn't either. The answer is I need the right number of  
6 credentials for the environments I'm working in and the  
7 interaction points I'm having. So I shouldn't have  
8 five cards that are all for the same environment. I  
9 want a limited number of ways to say, how do I make  
10 this efficient, how do I make this effective for the  
11 type of transaction I'm having or incurring. So  
12 we want to say, look for environments to say, how do I  
13 reuse what somebody already has.

14 The third one, inconsistency in vetting  
15 processes for like programs and revetting of the same  
16 individuals who were just seen. This is one of the  
17 ones that I know I care about very deeply and I'm sure  
18 you care about very deeply. It's what are the  
19 decisions people make as they're standing up these  
20 programs about which data sources to put that against?  
21 What's the accuracy level for those data sets? How do  
22 we choose which ones got there? How do we get one

1 either nominated to that or de-nominated from that data  
2 set? Is there a well understood process around it? Is  
3 there a way to correct the data set that's well  
4 understood?

5 All those things play into the fact that we  
6 were having programs with similar types of risks, but  
7 they were vetting against different data sources and  
8 often getting different results. And people would look  
9 at each other across the table, going, why did you find  
10 that and I didn't find that, or why do you think this?

11 Then the last problem we really identified  
12 was reliance on visual inspection. We would go through  
13 all these efforts to collect information, to conduct  
14 the vetting and issue these tamper-resistant cards, and  
15 then they were being used as flash passes, kind of not  
16 really the point. If you only had to do certain things  
17 up to a certain point and you could defeat the system  
18 by just looking like the person on the card, you're not  
19 achieving your security objective.

20 So we really said we need to move to a  
21 different environment. One has to be able to design  
22 credentials to support multiple licenses, privilege, or

1 status based on the risks in which the environment will  
2 be used. An example of this is the global entry  
3 Trusted Traveler Program with CDP. You don't get a new  
4 credential. You use your existing passport, but you  
5 have to carry it anyway because that's how you get into  
6 the other country. We just notate it in our system  
7 that, oh, they have this passport, this person is  
8 registered in the Trusted Traveler Program, they've  
9 undergone all the vetting. That's an example.

10 Design enrollment platforms and data  
11 collection instruments so they can be reused. Examples  
12 here are, as we are standing up each program each  
13 program says, oh, I have to call these people in, I  
14 have to collect biographic information, I have to  
15 collect biometrics. So if I'm USCIS, I have 130  
16 application support centers. I'm TSA, I have 100 TWIC  
17 locations. And guess what, they're in the same  
18 shopping mall right next to each other.

19 Inherently, we want to look for ways at DHS  
20 to say, how can we reuse our infrastructure in a way  
21 that makes sense.

22 Vetting associated with like uses and like

1 risks should be the same.

2 Entitlements to a license, privilege, or  
3 status, including immigration status, should be  
4 verified electronically.

5 Then the last one in here, very critical to  
6 us, that we ensure that there are opportunities for  
7 redress, that individuals are able to correct the  
8 information held about them.

9 The next step in going forward, because we  
10 said, well, these are kind of motherhood and apple pie,  
11 great statements, who's going to argue with some of  
12 these, is now we need to set a series of capabilities  
13 around these activities and we will drive to the next  
14 level to help people understand where are we going from  
15 here. Back again to, because there's no one right  
16 answer -- I can't tell you how many times I was in a  
17 room and people were trying to say, my way of doing  
18 intake is the best, the only way. The answer of course  
19 is there's not 157 right ways, but one is not the right  
20 answer.

21 So what we tried to do is say, we're going to  
22 come up with a range of options within each of these

1 steps within what we consider the credentialing-  
2 screening life cycle. And you're going to pick from  
3 these depending on what is your authority of your  
4 program, who are you interacting with, what are the  
5 other considerations around it, so I can make the right  
6 choices.

7 I hope you all noticed, there's no horizontal  
8 line. We did not want remotely it to look like there  
9 was levels, that this level was better than this one,  
10 because they are alternatives and they're acceptable  
11 alternatives. So for example, on the eligibility  
12 vetting and risk assessment, the second one, if your  
13 authority says that you should be doing a broad-scope  
14 terrorism, criminality, immigration, and identity  
15 verification, that's very different than if your  
16 enabling authority is, I just want to make sure the  
17 person is sponsored into this program. That one, for  
18 example, would be first responder. What is the primary  
19 requirement for a first responder? It's that he's the  
20 EMT employed by Arlington County. That's his  
21 requirements, that's a sponsor.

22 As opposed to some other program may be, my

1     only requirement, my only allowance is to do a  
2     terrorism check. So it's how do I make sure that I'm  
3     able to pick the right one. That one's a perfect  
4     example. This one can have levels in it. Obviously,  
5     broad scope would be broader than limited scope. But  
6     they could be paired with sponsored, approved, or not.  
7     You may have no requirement for a sponsor, or you could  
8     also have a requirement.

9             Another one I wanted to call attention to  
10    here is the redress-waiver column. As we look across  
11    setting up these standard requirements, we wanted to  
12    also say we need a standard way of thinking about the  
13    ability to intake information, make determinations  
14    around misidentifications or waivability of the  
15    information we found, and try to line up the policies  
16    around these.

17            So just like we want to get to an environment  
18    so we say you can respect a determination that this is  
19    the John Smith who's on the terrorist screening watch  
20    list, we want to get to a process where we can say you  
21    can respect the fact that they already decided that's  
22    not the John Smith who's on the terrorist screening

1 watch list, and be able to do that in a meaningful way  
2 across DHS programs.

3 As you would expect, all this is hard. It is  
4 detailed policy process discussions. These are not get  
5 to it in short amounts of time, and a lot of it is a  
6 big culture change. Very many of our components and  
7 our officers unfortunately often feel isolated, that  
8 they are kind of the last man at the gate, and  
9 especially, frankly, after 9/11, where so many  
10 individual officers were called out as letting someone  
11 through. Their risk aversion is high.

12 So getting to an environment where they can  
13 respect each other is very important for them to  
14 understand what happens before them, what happens after  
15 them, how are they integrating along the chain. That  
16 itself takes a significant amount of time.

17 On our next slide, we'd also like to focus in  
18 terms of thinking in our environments. This goes back  
19 to the whole, where should we make sure that like  
20 things work in a like manner. So we try to say let's  
21 look at how we need to harmonize within an environment,  
22 so that the same person's being encountered several

1 times within an environment, let's make sure that the  
2 outside person looking in goes, gosh, that makes no  
3 sense that you did these two things in these completely  
4 opposite ways. They need to make sense together.

5 So obviously, documents that we are issuing  
6 that are all about crossing the border should work with  
7 the technology that we're going to use when the person  
8 comes in the border. Things like, if we're going to  
9 have a process by which the air carriers are  
10 transmitting information into DHS for both Secure  
11 Flight for TSA for terrorism screening and for CBP for  
12 border processing, we want the carriers not to be  
13 receiving conflicting instructions, conflicting  
14 messages, conflicting processes, conflicting  
15 technology.

16 We want it to make sense, and we want a clear  
17 understanding both inside DHS about roles and  
18 responsibilities and how we communicate out about how  
19 is this information being used, is it going to both TSA  
20 and CBP, is it just being used by one, how is it held,  
21 who's got it, how long are they holding it, all those  
22 different cases?

1           So that's just one example. Access control  
2 is another environment. In general, in that  
3 environment we are -- unlike the border environment,  
4 where it really is a government-owned and operated  
5 environment, the access control environment, we're  
6 mostly dealing with transportation-critical  
7 infrastructure, where it's municipally owned, privately  
8 owned. We are in a completely different relationship  
9 with the people performing the checks, who are  
10 controlling the premises, and we really look there at  
11 more of a role of saying, what's the standard around  
12 the screening that's happening, what's the standard we  
13 can accept and build to so that they can have that  
14 respect for each other's credentials, understanding  
15 what the common screening process that was done, less  
16 so than us managing all of it directly.

17           Along those lines, we spend a lot of time  
18 talking about documents. The reason we talk about  
19 documents is you need to have a good chain of process  
20 of how a document was issued to have confidence that  
21 when you conduct a screening there was meaning behind  
22 the identity you're screening against. If you're using

1 a document that did not have integrity in the process,  
2 you could be running Mickey Mouse, and I can tell you  
3 he has not been arrested.

4 But you look at these other environments and  
5 you say, how do I make sense, how do I look at this and  
6 say, what's the way I want to look across these? So  
7 both they need to make sense in the environment they're  
8 in, but there's also some common threads that we want  
9 to see repeated in terms of how was the identity  
10 demonstrated, how is the document verified, am I able  
11 to verify it back with the issuing source so that I  
12 know, yes, State Department really issued this  
13 passport, State Department says this has not been  
14 revoked, and look, the data from State has this photo,  
15 which still matches the photo on the document, which  
16 matches the person standing in front of me.

17 How do we set up these types of transactions  
18 so that we're not in that flash pass environment? So  
19 you'll see here some of the examples of recent efforts.

20 Then I think I'm almost down to the end of  
21 the slides.

22 Biometrics is another area where we have

1 looked to try to really push towards a common set of  
2 strategies and policies. In part, we focus on the  
3 People Screening Capstone Integrated Project Team run  
4 by Science and Technology. You've probably had a  
5 briefing on the Capstone process. No? You need a  
6 briefing on the Capstone process.

7           The great thing about this process is it  
8 brings in the various mission owners and says, identify  
9 your core gaps, what are the things out there, your  
10 mission gaps, your mission needs, that you aren't able  
11 to achieve today, and then what's the research and  
12 development priority component of achieving those gaps?  
13 Not the whole gap and not a gap that you can satisfy by  
14 existing technology, but what's the research and  
15 development aspect.

16           It's a great way to really make sure that  
17 they're focusing the limited number of dollars on those  
18 gaps that more than one component has, that more than  
19 one component is facing.

20           We have also established as one of the DHS  
21 services the biometric storage and matching service of  
22 IDENT. That's another one where we focused.

1           Then the third one, of course, is focusing  
2           with U.S. VISIT on the interoperability between IDENT  
3           and IAFIS.

4           The last slide I wanted to briefly talk about  
5           is redress, and in particular the DHS TRIP program. As  
6           you see here, it's kind of a work flow process for how  
7           it works. I know you've had a couple briefings from  
8           Jim Kennedy. I probably won't step through the  
9           process. The key really from our perspective is how do  
10          we make it as easy as possible for people to submit  
11          while still making sure that we're not giving  
12          information back to somebody that's not them, that  
13          we're able to resolve issues, that we use this  
14          opportunity to look at the records that we're using for  
15          screening, to say, if I can really say it's not that  
16          Jim Smith how do we fix that issue so it stops  
17          happening in the future. If Jim Smith should not be on  
18          the watch list, which agencies do we have to talk to to  
19          get that remedied?

20          And as you would expect, back to again, in  
21          certain areas this works very quickly and very fast,  
22          and other places it's like, oh gosh, we haven't talked

1 to that agency in quite a while and we need to work out  
2 additional policies and procedures on how to make this  
3 work more effectively into the future.

4 Our job -- Jim's job, is to make sure all  
5 paper goes in and out. Our job is to look across some  
6 of this and say, is this working like we wanted it to?  
7 Where are there opportunities for improvement? Is it a  
8 resource issue, because Jim doesn't have enough people?  
9 Is it a components not -- we've had too many  
10 changeovers in an office, too many people change over,  
11 and they forgot where the priority fell or how this  
12 works in the greater scheme? What's out there that we  
13 need to address and push forward?

14 I just want to correct the one number on  
15 there. It says "received 58,500 complete cases since  
16 February 2009." That's since February 2007. Sorry  
17 about that.

18 And note that that's 58,500 complete cases.  
19 The case came and we have all the materials we needed  
20 to actually resolve it. For cases where the person  
21 never followed up with providing the additional  
22 supplemental documentation, that is not included in

1 those numbers.

2 That's all my slides. So I'm sure you're  
3 going to have lots of questions.

4 CHAIRMAN PURCELL: Thank you, Ms. Cogswell,  
5 for both a refresher course on screening coordination,  
6 but also a refreshing review of progress made over the  
7 last couple of years.

8 I'll call first on Charles.

9 MR. PALMER: Agreed. Thank you very much,  
10 and I particularly appreciate your enthusiasm and  
11 interest to resolve this. Everybody wants to solve  
12 problems, but wow.

13 As one of the geeks here, I'm immediately  
14 interested in your advice. You advise and direct  
15 components on how to solve their missions, either using  
16 technology or not. I have two questions. This is the  
17 first part of the first question: Do you advise and  
18 attempt to coordinate those so that they do play nice  
19 into the future? Some of my experience has been these  
20 guys and gals are doing the best they can, working as  
21 fast as they can, with what money they have, to solve a  
22 problem that is not always optimum. That's the first

1 question.

2 MS. COGSWELL: So the first question is do we  
3 advise, coordinate, and -- there was a third term I've  
4 forgotten already. Anyway, the answer is yes. As you  
5 highlighted, sometimes we have more options in an area  
6 than others. Sometimes that isn't an area that has a  
7 lot of funding, so you say, what are my near-term  
8 options that I can achieve in the funding I have, but  
9 no one forget where we want to go.

10 So for example, when I laid out that  
11 capability set, one of the things that we very quickly  
12 noted was our office, we don't have a budget. We can't  
13 pay anybody to build things. We need to look to the  
14 components to say, where are you already receiving  
15 dollars, where are you already expected to do maybe 80  
16 percent of something anyway, and can we look to  
17 leverage that funding to add in this other bit that  
18 otherwise you, CPB, might not care about, but makes a  
19 huge benefit for these three other agencies, as an  
20 example.

21 So yes, we work extremely closely with the  
22 components as they're actually implementing. This is

1 something that our office does that is very  
2 unconventional, I think, for a policy office, to be  
3 this involved with actual implementation and operation  
4 of a program.

5 I will say, no surprise to you, certain  
6 components are very accustomed to working with us and  
7 work extremely closely with us. Other components are  
8 still going: Scope? So we do not have an equal  
9 relationship in every place.

10 MR. PALMER: Thank you. The second question  
11 is, I didn't hear the "international" word. How much  
12 of this coordination is actually done with colleagues  
13 elsewhere?

14 MS. COGSWELL: Oh, very good question. Some  
15 of it's a lot and some of it is -- for example, where  
16 we have bilateral relationships with different  
17 countries, for example the United Kingdom, we have a  
18 regular process in which we sit down, DHS, with our  
19 counterparts in the U.K. We're able to share best  
20 practices. So for example, we went through a process  
21 where we said, this is kind of the problem set we're  
22 seeing and some of the solutions we're identifying; are

1     you encountering similar problems? Are you heading  
2     toward the same sort of strategic solutions that we're  
3     talking about? And the answer was yes. They said:  
4     Gosh, ours is much less complicated and convoluted than  
5     yours, and we're very happy that you guys have more  
6     problems than we do.

7             But generally speaking, we have some good  
8     opportunities through international relations to also  
9     say, have you had a particular success in an area in  
10    this range that potentially we can look to to leverage  
11    or use as well? And then obviously we work extremely  
12    closely with the components for doing any kind of  
13    international information exchange for derogatory  
14    information that may be used in screening.

15            MR. PALMER: Thank you.

16            CHAIRMAN PURCELL: Thank you.

17            Mr. Sabo.

18            MR. SABO: Thanks.

19            Just a question on -- you're housed in the  
20    Office of Policy and a lot of the great things you're  
21    doing is focused on better integration of technologies  
22    and practices and efficiency. But one of your roles

1     apparently is this overarching framework of policy  
2     development, strategic oversight.  Back in 2006 this  
3     committee developed and issued a report on the  
4     framework for assessing the privacy impacts of programs  
5     and policies.  One of the issue areas was efficacy.  In  
6     other words, to some extent it's things you talk about,  
7     which is risk management:  What's the cost of a  
8     program, how effective is it, and what is the impact of  
9     that cost against individual privacy and liberty and so  
10    on?

11            So my question is, are you involved at all or  
12    is there work involved in your office or anywhere in  
13    the Office of Policy in looking at that risk assessment  
14    from that perspective?  In other words, we're spending  
15    billions -- as an example, we're spending billions to  
16    do screening at airports, including identity screening;  
17    what's the value of identity screening in preventing a  
18    particular use of that airplane for terrorist purposes,  
19    for example?

20            Do you get to that level of questioning or  
21    data analysis or studies which would look at the bigger  
22    value of a program against the risks against the costs.

1 And if you were, can you talk about some initiatives  
2 that you have under way to address that?

3 MS. COGSWELL: The answer I'm going to give  
4 you is we have a lot of interaction, especially on the  
5 front end of the program when it's first being set up:  
6 What is my objective? What are my options, to really  
7 be able to look at, are the dollars I'm spending likely  
8 to turn into a positive result and be worth the  
9 dollars? We have less impact and visibility on the,  
10 okay, now it's been implemented for a year, let's see  
11 if the results are living up to the promises, in many  
12 places, than I think we'd like.

13 So with that said, on the up-front side  
14 there's an investment management process that DHS is  
15 using. I don't know if you've had a briefing on MD-  
16 1400? No, okay. But a lot of the up-front pieces are  
17 things like how do I articulate what my mission need  
18 is, how do I articulate what my operational  
19 requirements are? When I design my solution, how am I  
20 making sure that the solution ties directly back to  
21 those requirements I stated? How am I measuring how  
22 much of the outcome actually solves the problem I set

1 out?

2 There's a rigorous process on that front, and  
3 then as you implement the next stages. DHS does not  
4 have as robust a process at this time of the back-end  
5 follow-up.

6 MR. SABO: Who would be responsible for that  
7 follow-up process? Would that be the Office of Policy?  
8 From a screening perspective, does that fall to your  
9 office?

10 MS. COGSWELL: If it were a screening  
11 program, yes, it would fall into our office. I would  
12 say that there's a couple pieces to that. Just like we  
13 have a process that people follow on the front end  
14 getting the investment, in order to make it meaningful  
15 what we'd really like is a similar process for people  
16 to follow on the back end. In other words, what  
17 happens right now is where there's an individual  
18 program who chooses to do it or is required to do it  
19 because of their appropriations or because of GAO, we  
20 can get involved there. But there's not that  
21 consistent requirement on the programs across the  
22 board in the same way.

1           So I think we would look to from a more  
2           strategic policy matter say, how do we make sure that  
3           we are doing the back end of the feedback loop. So  
4           that would be the piece where I would see us partnering  
5           with the Office of Management, specifically the  
6           Acquisition Program Management Division, who's  
7           responsible for establishing some of these investment  
8           review processes.

9           MR. PALMER: It's not like there's a policy  
10          in place --

11          MS. COGSWELL: It's not consistent and it's  
12          not across the board.

13          CHAIRMAN PURCELL: Through a series of miming  
14          actions, I'm going to take Jim's question next, which  
15          is related apparently.

16          MR. HARPER: I was unable to indicate, using  
17          American sign language or any other, that my question  
18          was closely related to John's, so I wanted to just  
19          follow on. Thank you, Mr. Chairman.

20          CHAIRMAN PURCELL: Certainly.

21          MR. HARPER: I would have asked the same  
22          thing, but just raising it in terms of the Results Act:

1 Do you do Results Act reporting or do you collect the  
2 Results Act reporting of the organizations that you  
3 coordinate, because I think that would be a great  
4 insight for Congress as to the value that they provide  
5 for the American taxpayer.

6 MS. COGSWELL: We do not set the  
7 requirements, nor do we do the actual reporting. The  
8 Office of Management is in charge of that process. We  
9 do get to see the results as part of that process and  
10 obviously have the opportunity to work with the  
11 components through that process and say, is this the  
12 right metric.

13 In particular, the big place we also get to  
14 impact is budget. So if I have a series of metrics  
15 that are showing these kinds of things and I have to  
16 recommend what dollars will be spent for the next year,  
17 we're going to look for the places where you're making  
18 the best investment for the dollars.

19 MR. HARPER: So the easier metrics are number  
20 of people screened or tonnage of cargo screened. Those  
21 are process metrics. Do you have actual results  
22 metrics, which would be harm to the country avoided,

1 things like that, which are hard to do?

2 MS. COGSWELL: They're very hard to do. It's  
3 something the Department's been working on for a couple  
4 of years, and I do not feel that we have great examples  
5 in that arena that are cross-cutting metrics. There  
6 are individual program metrics, which is not what you  
7 want.

8 MR. HARPER: Thanks.

9 CHAIRMAN PURCELL: Thank you.

10 So back to our order: Ramon, and as  
11 concisely as we can.

12 MR. BARQUIN: As concisely as I can, two  
13 questions. First of all, in terms of redress, I think  
14 the largest -- I know part of your graph is TRIP, which  
15 we just got a little bit of a briefing on before. But  
16 there is certainly the need for redress beyond travel.  
17 I just wanted to see how you're dealing with that.

18 The second is that, again I think we all know  
19 the shortcomings of the breeder documents, the social  
20 security numbers and so forth. Could you give us a  
21 sense of, in this reality show that you've got to deal  
22 with with all these documents, what kind of progress

1 have you made with biometrics or other things to try  
2 and address those shortcomings?

3 MS. COGSWELL: That's a great question. The  
4 first one, redress beyond travel. Yes, it's definitely  
5 something that we care about very deeply, and we are  
6 looking at various options on trying to approach that.  
7 One of the easy ones to focus in on because it's  
8 related to travel is transportation programs. They're  
9 not travelers, but they're working in the  
10 transportation industry.

11 There are additional groupings as well. Any  
12 time you talk about critical infrastructure, some of  
13 those arenas, and where we're talking about standing up  
14 big programs you want to immediately accompany it with  
15 the ability to redress.

16 As you expect, we have very interesting  
17 balancing acts. So on the one hand you want to make it  
18 as easy and open as possible for people. On the other  
19 hand, by definition these are a majority of people who  
20 are not bad actors, so how do I protect their  
21 information by not taking the John Smith who's not the  
22 terrorist and sharing his information? And how do I

1 avoid confusing people, who think they applied to one  
2 program for one activity? I need to tell them you can  
3 authorize your information for use in another arena.  
4 We want to be as open and transparent as possible.

5 So it's definitely something we have a large  
6 interest in doing and we're weighing through a number  
7 of the, how do you make this happen in a meaningful way  
8 that people will respect the openness and the  
9 transparency of the process.

10 Number two, documents. You're right. I love  
11 that, a reality show. That's a great comment.

12 We have seen a lot of progress. There's a  
13 couple places that people tend to focus on. I like to  
14 focus in part on the, what was the process that went  
15 into the issuance? Do I have a confidence that the  
16 people who were the ones taking the information, the  
17 ones who vetted the information, someone who printed  
18 the card, that is not a process that could be easily  
19 suborned, that I don't feel like I could describe one  
20 person and you got a credential. It can have the best  
21 biometrics on the planet on it and it's still --  
22 there's no integrity in the issuance.

1           Basic things like, is this a process where  
2 they secure the materials so that you can't just steal  
3 them, or it's not a printer that somebody can just buy.  
4 Those type of things help you have some confidence in  
5 the process.

6           Biometrics are an area that I have interacted  
7 with people with a range of viewpoints on that one.  
8 Photographs in many ways are a biometric that people  
9 understand the most and are used to dealing with, and  
10 one also people will say, well, you show your face all  
11 the time, you have an expectation that it's out in the  
12 public domain. On the other hand, certainly people for  
13 religious reasons that is the worst biometric to deal  
14 with, so they want that one protected.

15           I would also say, from the technology  
16 perspective, of our big three of biometrics, which is  
17 face, fingerprint, and iris, face is struggling the  
18 most in the automated recognition capability, because  
19 of time. It's harder to match you over time, and the  
20 conditions in which the collection occurred affect the  
21 matching so much. When we talk about a biometric we  
22 like it to be something where there's the least amount

1 of discretion, so that the machines largely make the  
2 match, a very trained person makes the match, not just  
3 the subjective, is that the same person.

4 But frankly, the way face works, depending on  
5 how it was collected and how big a gallery you're  
6 matching against, humans do very well in comparison to  
7 machines. So that's a problem.

8 Fingerprints, much higher quality, much more  
9 mature technology, still a lot of concerns today about  
10 if you collect fingerprints does that mean  
11 automatically everything is going to be checked against  
12 criminal history records, and I thought I was getting  
13 my fingerprints for my child's safety and instead it's  
14 now put into some criminal history database. There are  
15 a lot of concerns around that, because the tradition of  
16 fingerprinting was really around the criminal history.

17 Iris, of course, is the new kid on the block,  
18 so to speak. Lots of promise coming, but still  
19 struggling from its proprietary roots to have that kind  
20 of vendor-neutral environment. I think that's an area  
21 that's going to continue to grow, not the least of  
22 which is it has that -- people have a lot of excitement

1 around that because of the ability to remove the  
2 subjectivity around an identity. They like the idea  
3 that it's not -- I don't have to make a judgment.

4 But it has to be partnered with there was  
5 integrity in the process that linked the biometric with  
6 the identity. Otherwise -- so a long way around. Did  
7 I answer your question?

8 CHAIRMAN PURCELL: Accountability in the  
9 process is just as important as the taking of it.

10 MS. COGSWELL: Very much so.

11 CHAIRMAN PURCELL: Quickly, Ms. McNabb. We  
12 are over time at this moment, so I'm going to try and  
13 actually take the questions, but your discipline is  
14 going to be required, too.

15 Ms. McNABB: I have a short question. How  
16 well are you doing in working on redress with the  
17 nominating agencies?

18 MS. COGSWELL: Very good question. There is  
19 a very well understood process around the terrorist  
20 functions. Everybody's signed up to an MOU. There is  
21 a detailed process. There is an understanding about  
22 what the requirements are to get on the terrorist watch

1 list. I am so pleased when I go into places and  
2 they're asking me questions like, hey, I know you guys  
3 put this guy on the list because he was a reporter who  
4 said something critical about the United States.  
5 Absolutely not; I know what the criteria for getting on  
6 the watch list is, and that ain't it; he wouldn't  
7 qualify.

8 I very much appreciate how much a culture  
9 change it's been to get to that point for the  
10 nominating agencies, in particular to open up their  
11 process. I think we always have more room to go in  
12 that area, but gosh, compared to just a couple years  
13 ago we are so light years ahead in terms of us even  
14 being able to communicate in a standard language.

15 Other areas, I would like to see us mature a  
16 lot more. I think everybody is well aware that the  
17 process by which a law enforcement agency in this  
18 country may nominate someone for a warrant -- there's  
19 different criteria. Things like, okay, I will nominate  
20 them for the warrant, but I'm only going to extradite  
21 in these five states. So it's an uneven process where  
22 there's not the same, there's one sheriff and he

1       answers the phone. So it's not the same robust  
2       process that we've gotten used to expecting in this  
3       other area.

4               I have a tendency to keep trying to push more  
5       into the environment where you can say, I have that  
6       guaranteed 24-7 ability to call to find out information  
7       that I don't have, so I can make the right decision and  
8       not just hold somebody. And I think we're going to  
9       continue to keep needing to mature these.

10              CHAIRMAN PURCELL: Neville.

11              MR. PATTINSON: Thank you.

12              One quick point and then a question. I'm  
13       very glad to hear about the new biometrics as an  
14       identifier. It's an attribute that can be used to help  
15       the process of identification. I think from a  
16       biometrics perspective, one to many is still an area of  
17       continuous improvement, but I think one to one is  
18       something where biometrics can add value.

19              One area that I'm seeing discussion around at  
20       the moment is at airports and credentialing at  
21       airports. I think your office holds a key position in  
22       really the policy and the strategy as this goes

1 forward. There's the specification floating around.  
2 Then I see lots of different communities concerned  
3 about how do they get access to airports -- federal air  
4 marshals, airport employees, the list goes on, first  
5 responders.

6 So how do we address all these perspectives  
7 on the access control to the airport? The officers  
8 have their physical domain. They're in charge, so to  
9 speak. But there needs to be, I think, a terrific role  
10 that your group can take in guiding the whole  
11 facilitation and coordination of how an airport has its  
12 control done and how that information is then  
13 transferred from those credentialing systems to effect  
14 that system.

15 I think this is an area that your office has  
16 a terrific mission ahead of it. That's certainly  
17 something we're seeing at the moment, with  
18 proliferation of credentials. If you're a person that  
19 likes a proliferation of credentials, fine. But it's a  
20 question of they all need to be vetted and  
21 authenticated.

22 So I'd be interested to know if you're

1 working at all with TSA or in the airport environment,  
2 around that complex area.

3 MS. COGSWELL: The answer is absolutely.  
4 Specifically, the TTAC organization, Transportation  
5 Threat and Credentialing Unit, runs the vast majority  
6 of those types of programs. This is something they  
7 very well recognize and acknowledge. I love when --  
8 and maybe it would be another one for your future  
9 agenda list -- they have kind of a modernization effort  
10 under way that maybe would be good for you to hear  
11 about, in terms of where some of their thoughts are to  
12 try to harmonize a lot of their programs.

13 Back to your point, though, of all right,  
14 this guy, I just badged him for airport access and then  
15 I'm going to badge him again for this other process,  
16 but it's the same information; how do I make this a  
17 reuse? It's the same credentials, the same  
18 specification. I just need to be enrolled in this  
19 other access system, as opposed to starting over from  
20 scratch.

21 I think that would be great to potentially  
22 have on your future agenda. And yes, we work extremely

1 closely with them to try to help make that.

2 One of the areas I think we're most working  
3 towards is, any time you're talking about a distributed  
4 environment, which I think we all see many benefits in,  
5 it does mean you have an immensely larger number of  
6 stakeholders to work with, and you have to keep  
7 communicating with on a regular basis. That's an area  
8 I know we've struggled sometimes, on how do you keep  
9 all those hundreds of facilities engaged, involved,  
10 marching in the same direction, on the same time line?  
11 They're sometimes competitive. Disadvantages to be the  
12 first adopter in an area, so how do we help make those  
13 environments work when you've got such a distributed  
14 acquisition and implementation model?

15 CHAIRMAN PURCELL: At the risk of annoying  
16 Martha further, I'm going to take one more question.  
17 I'm going to defer to Howard, whom we haven't heard  
18 from yet today.

19 MR. BEALES: I wanted to ask about the  
20 redress numbers. I guess probably three parts to this  
21 question. One is, what's the mix of problems that are  
22 watch list problems versus identification problems

1 versus misidentification, mismatch problems?

2 Two is, where do these -- you've got this  
3 graphic of where the complaints come from across  
4 different agencies, and I'm wondering if there are  
5 differences other than the volumes obviously different  
6 across these programs. But are there differences other  
7 than that in problems?

8 Three is, what's the story on the 11 percent  
9 of cases that are still open, or is that just the flow  
10 of new complaints coming in that aren't yet complete  
11 and therefore aren't yet done?

12 MS. COGSWELL: In order to help answer some  
13 of these, I'm going to invite my colleague Ted Sobel  
14 up. He works day in and day out with a lot of these  
15 numbers, so I think he can help on these.

16 Do you want to start with the first one, on  
17 the watch, actual watch issues?

18 MR. SOBEL: Sure. Actually, there was a  
19 third category in there. It's not just your watch list  
20 or your misidentification. You can also be applying  
21 through DHS TRIP for a non-watch list-related issue.  
22 Obviously, you as a member of the public don't know

1 that. You just know what your screening experience is.  
2 You don't know the reason why. So you're applying to  
3 DHS TRIP and saying, I'm getting stuff or I'm getting  
4 additional screening each time I travel; what can you  
5 do about it? So that's the third category.

6 Examples of that third category would be  
7 immigration visa overstays, things like that, that  
8 again are reasons that we would get additional  
9 screening, but it's not watch list and it's not  
10 misidentification.

11 So with that third category in mind, you have  
12 about two-thirds of our volume is TSA, is domestic  
13 travel. Over 98 percent of those probably fall into  
14 the misidentification category. The exact numbers are  
15 I believe classified, so we can get them in a different  
16 environment. So two-thirds, basically two-thirds are  
17 misidentification related. A small sliver of that is  
18 actually watch list-related. Those we work in  
19 coordination with the Terrorist Screening Center.

20 Then about one-third are all the other  
21 agencies, all the other offices besides TSA -- State  
22 Department, Customs, ICE, etcetera. Those for the most

1 part are not watch list issues and for the most part  
2 those are not misidentifications. Probably somewhere 20  
3 percent or so of those are misidentifications. For the  
4 most part, they are real issues that need to be worked  
5 differently.

6 In terms of the cases in process, yes, those  
7 are the ones that are currently being worked. For the  
8 most part, they're the more recent cases. We have  
9 about -- overall in our system, it takes us about 60 to  
10 75 days to work a case. That's a median. There are  
11 clearly cases that have taken longer, and depending on  
12 the complexity of the case it takes longer. So if it's  
13 a watch list or a misidentification, those actually  
14 tend to be worked very quickly because we can narrow it  
15 specifically. If it's something that's going to, say,  
16 CBP or through privacy because they have some sort of  
17 complaint where they think information was misused,  
18 those will take longer because there's a lot more labor  
19 hours and a lot more intensive work that's needed to be  
20 resolved.

21 MR. BEALES: What's the clearance rate for,  
22 like if you looked at the complaints between February

1 of '07 and February of '08? One would hope we've  
2 mostly cleared those, but how well have we done?

3 MR. SOBEL: What is your criteria for "how  
4 well"?

5 MR. BEALES: Just closing.

6 MR. SOBEL: Closing, we're at probably 97, 98  
7 percent closed from those older ones.

8 MR. BEALES: So there's a long tail of old  
9 ones that hang on for quite a while?

10 MR. SOBEL: Yes, because they're the ones  
11 that -- for the most part, they're either requiring a  
12 lot of work or they have a lot of components that are  
13 brought in. One of the advantages of DHS TRIP we give  
14 to the public over the preexisting system is one  
15 application, many agencies. So if you've got a  
16 problem, especially if you don't know what the problem  
17 is, with multiple agencies, we will keep working it  
18 until we get it all resolved, all the boxes checked.

19 MR. BEALES: Just a last little part, if I  
20 might, on the problems. On the watch list issues that  
21 are really watch list, and maybe there aren't enough to  
22 answer this question, but are there patterns among the

1 nominating agencies as to where there are issues?

2 MR. SOBEL: I don't think -- as you said, I  
3 don't think there is enough of those sort of cases that  
4 we'd be able to discern it.

5 MR. BEALES: Okay.

6 MR. SOBEL: That is something we do look for  
7 and consult with TSA to get additional information.  
8 But I'm not aware of any particular pattern.

9 CHAIRMAN PURCELL: Ms. Cogswell, thank you  
10 very much. Ted, thank you for helping out. We  
11 appreciate your time with us today; very, very helpful.

12 As we set up for Mr. Gersten next quickly, I  
13 want to remind the public that the opportunity to  
14 address your comments to the committee will be  
15 immediately following this next presentation, and the  
16 sign-up sheet is in the back. Do we have sign-ups, so  
17 we can manage time against the number of people, the  
18 hordes of citizens who are clamoring for a chance to  
19 address the committee?

20 (Pause.)

21 CHAIRMAN PURCELL: I'd like to welcome David  
22 Gersten now to the committee. Hello. How are you,

1 David?

2 David is serving as the Acting Officer for  
3 Programs and Compliance in DHS Office for Civil Rights  
4 and Civil Liberties. He has also served in that same  
5 office in the CRCL Programs Division as the Director.  
6 Before joining DHS, I'm told that Mr. Gersten led the  
7 customer service efforts for the U.S. Department of  
8 Education Office of Civil Rights and served also as the  
9 Executive Director of the Center for Equal Opportunity.

10 Mr. Gersten, welcome.

11 DHS OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES UPDATE,

12 BY DAVID D. GERSTEN

13 MR. GERSTEN: Thank you so much. I'm very  
14 pleased to be here. I think I have helped to address  
15 you many times on various subjects. Our prior officer,  
16 Daniel Sutherland, came before you a little over a year  
17 ago to discuss our civil liberties impact assessment  
18 program, and I'm very pleased to give you an update on  
19 that program and in particular discuss one impact  
20 assessment that we're conducting now on the border  
21 search of electronic devices.

22 I also know that you heard from one of our

1 staff just in recent months, George Selim, who helps to  
2 conduct our community engagement with American Arab  
3 Muslims, Sikhs, and South Asian community members. He  
4 told me he was very pleased with the input that you  
5 provided and with the exchange that he had, and the  
6 community members were also very pleased. He continues  
7 to have his dialogue with community members in Detroit  
8 and we also have round tables around the country and  
9 they are very interested in continuing to have some  
10 interaction with all of you.

11 An overview of the civil liberties impact  
12 assessment. I think you all have slides in front of  
13 you. You can all be referring to them. There is one  
14 correction and I'll mention that as we go forward.

15 We've been conducting civil liberties impact  
16 assessments ever since the 9/11 Act called on our  
17 office to examine four particular Information Sharing  
18 Environment programs. We have expanded the program to  
19 be a proactive program to conduct impact assessments  
20 when senior leaders in the Department or program  
21 managers themselves are interested in having a review  
22 of how a program might impact individuals or even other

1 entities and compare those programs with the Bill of  
2 Rights and other statutory rights that we all hold  
3 dear.

4 One of the programs that has been under way  
5 for many years, but has been recently updated, is the  
6 policy of border search of electronic devices. The  
7 Department has long held that -- and the Secretary  
8 announced that directives on border searches needed  
9 some updating and she, Secretary Napolitano, updated  
10 the border search policies in August of 2009. CBP and  
11 ICE directives are meant to enhance transparency by  
12 publicly releasing CBP and ICE directives.

13 We were charged in that announcement of the  
14 release of the directives to conduct an impact  
15 assessment. I'll get to that, get back to that, in a  
16 minute. But I just wanted to give you a preview of  
17 what I'll be talking about. So I'll be talking about  
18 the specific border search and electronic device impact  
19 assessment. I'll go over border search authorities and  
20 I'll discuss the CRCL analysis of the directives. Then  
21 I'd like some feedback from all of you on  
22 recommendations as we go forward.

1           CRCL receives its authority to conduct impact  
2 assessments, as I said, from the 9/11 Act, but also  
3 from its authorizing act, 6 U.S.C. 45, the Homeland  
4 Security Act of 2002, and the certification language of  
5 the Consolidated Appropriations Act of 2008, which  
6 called on us to conduct impact assessments of a few  
7 more programs.

8           The types of questions that we ask can be  
9 found online in our template, the annex to our first  
10 impact assessment on state and local fusion centers.  
11 But some of the ones that may be of particular use in  
12 our current impact assessment on border search of  
13 electronic media, we ask questions about whether or not  
14 there is public notice of the program and whether or  
15 not individuals have the ability to file complaints  
16 about the program; are procedures available for redress  
17 of alleged violations of civil rights and civil  
18 liberties, and if so how will the public be informed of  
19 these redress procedures; and also, do the redress  
20 procedures provide for data corrections to be sent to  
21 all of the entities with which the information has been  
22 shared.

1           We also ask whether or not the effective  
2     implementation of the program is dependent in whole or  
3     in part upon government employees having a heightened  
4     awareness of their constitutional rights and their  
5     responsibility in ensuring that those rights are  
6     respected; and also, of course, departmental policies  
7     as they carry out their duties.

8           Each individual impact assessment is  
9     different. We've conducted impact assessments on  
10    behavioral detection officers and their role in  
11    transportation screening, for instance, and looked  
12    quite a bit at the issue of whether or not race or  
13    ethnicity is used as a factor, while in an impact  
14    assessment related to information-sharing we tend to  
15    focus on respect for First Amendment rights, for  
16    instance.

17           With the border search of electronic devices,  
18    the two directives that we were primarily focusing on  
19    are the new ones that have been updated recently this  
20    August: the CBP Directive 33340-049, entitled "Border  
21    Search of Electronic Devices Containing Information,"  
22    and ICE Directive No. 7-6.1, entitled "Border Search of

1 Electronic Devices." These can be found online and  
2 I'm happy to facilitate making sure that you have a  
3 copy of them.

4 Our efforts to date have involved reaching  
5 out to private sector partners, coordinating with a  
6 number of advocacy organizations during the roll-out of  
7 these new directives to obtain some feedback, their  
8 initial reaction to the announcement of these new  
9 directives. We contacted the Brennan Center. We spoke  
10 with the Muslim advocates.

11 By and large, the private sector raised  
12 typical First Amendment concerns about content found on  
13 electronic devices being subject to officer scrutiny.  
14 They also -- some of the groups asked that we analyze  
15 how passengers are selected for review while crossing  
16 the border and determining whether or not there is any  
17 link to racially motivated scrutiny of any sort.

18 We've worked closely with CBP and ICE subject  
19 matter experts and conducted a comprehensive review of  
20 the border searches. We are working with our General  
21 Counsel's Office as well to provide a complete legal  
22 analysis of the directives, focusing specifically on

1 the Fourth Amendment and First Amendment concerns.

2 The announcement of the new policies stated  
3 that we would complete our impact assessment within 120  
4 days. We will have our impact assessment delivered to  
5 the Secretary the first week of January, which will  
6 mark about the 120-day mark.

7 Since it is not a statutorily required impact  
8 assessment, we will have to decide just how much of the  
9 impact assessment will be a public document. There are  
10 certain portions of our analysis that will of course be  
11 law enforcement sensitive. In fact, some of the  
12 analysis may be secret in that it involves the nature  
13 of the exploitation of electronic media. So that said,  
14 our intention is to at the very least provide an  
15 executive summary that will be publicly available.

16 Moving on to border search authority, border  
17 search authority predates the ratification of the U.S.  
18 Constitution. The first customs statute was passed two  
19 months prior to the ratification of the Constitution.  
20 Section 24 of the statute grants customs officials full  
21 power and authority to enter and search any ship or  
22 vessel in which they shall have reason to suspect any

1 goods, wares, or merchandise subject to duty shall be  
2 concealed.

3 Immigration -- CBP and ICE are charged with  
4 enforcing over 400 laws at the U.S. border involving  
5 immigration, immigration laws, the Immigration and  
6 Naturalization Act, customs laws, obviously related to  
7 preventing illegal contraband from entering the  
8 country, inadmissible agriculture, and then of course  
9 federal laws and regulations enforced at the border,  
10 restriction or prohibition of the flow of persons or  
11 merchandise crossing U.S. borders. Then prohibited  
12 contraband that may be interdicted at the border  
13 includes child pornography, evidence of commercial or  
14 financial crimes, evidence of infringements on  
15 copyright or trademark, evidence of human and bulk cash  
16 smuggling, physical or documentary evidence of  
17 violation of export controls, evidence related to  
18 terrorism and other national security concerns.

19 Customs officials seek to restrict or  
20 prohibit the flow of persons or goods that violate laws  
21 enforced at the border and all persons, goods, and  
22 containers are subject to search on entry and exit from

1 the U.S.

2 Just to give you a reference point on the  
3 volume, CBP is enforcing these laws as approximately  
4 260 million travelers cross the border each year.

5 Now, what do we mean when we say electronic  
6 devices? I have several of them on me right now -- a  
7 Blackberry, an iPod --- or iPhone, I should say --  
8 thumb drives, laptops. Electronic devices are  
9 considered analogous to containers. Electronic devices  
10 are equally subject to search for illegal contraband.

11 The CPB and ICE directives provide guidance  
12 and policy and procedures for searching electronic  
13 devices. We have evaluated the directives with an eye  
14 towards specific civil liberties issues. The  
15 directives build in certain civil liberties  
16 protections. As you'll see on the slide, they provide  
17 notice to passengers. This notice is in the form of a  
18 tear sheet that is handed out if an electronic devices  
19 is detained or seized. That tear sheet actually does  
20 reference our office and the Privacy Office,  
21 specifically stating that if a person -- in fact, I'll  
22 read it to you right now. The tear sheet states that:

1           "The DHS Office for Civil Rights and Civil  
2 Liberties investigates complaints alleging violations  
3 by DHS employees of an individual's civil rights or  
4 civil liberties," and additional information about our  
5 office can be found at our web site. There's a privacy  
6 and civil liberties protection section of that tear  
7 sheet.

8           So the new tear sheet is an improvement that  
9 we've seen in our analysis of the directives.

10           The directives also build in a protection by  
11 ensuring that the search is conducted, where  
12 appropriate, in the presence of the traveler. It also  
13 restricts the length of time for search of electronic  
14 devices where possible, and there are ICE policies and  
15 procedures that supplement the directive that explain  
16 just how the searches are prioritized.

17           It also requires, the new directives also  
18 require supervisory approval in certain instances, and,  
19 as I mentioned earlier, the new directives provide for  
20 information on filing a complaint.

21           All of that said, we are certainly  
22 identifying some areas for improvement. Technological

1 advances in electronic devices may raise new  
2 unanticipated civil liberties concerns. Certainly  
3 these concerns are raised repeatedly when the subject  
4 comes up. As we grow in capacity for what we can carry  
5 in an electronic device, we're of course containing a  
6 lot more information that we as individuals believe is  
7 privileged. So that's certainly an area of concern.

8           Also, another area of improvement is to  
9 ensure that training materials and procedures promote  
10 fair and consistent enforcement of law related to  
11 electronic devices. We have a strict policy in the  
12 Department prohibiting the use of race, prohibiting  
13 racial profiling of any sort, and that is certainly  
14 enforced. However, it ensures -- to ensure that it's  
15 carried out, that policy must be supplemented with  
16 regular training. So we continue to recommend in  
17 almost every impact assessment that training be  
18 enhanced to make sure that staff at our borders  
19 understand their responsibilities in ensuring  
20 compliance with our racial profiling policies.

21           We also identify one area of improvement of  
22 providing travelers with clear and concise material

1     informing them of the search, informing travelers of  
2     how their data may be used, and identifying the  
3     constitutional and statutory rights.

4             The Secretary's memo describing the  
5     initiative did in fact point to some of these future  
6     actions. She mentioned training for Customs Officers  
7     and information for passengers about the search.

8             With that, I'd like to open it up for  
9     questions. Please, if you have other questions about  
10    our work, I'm happy to answer them. I almost felt an  
11    urge to answer one of the questions that you asked  
12    Patty Cogswell, Joanne. You mentioned redress on the  
13    back end. One bit of news I'll report, that we are  
14    happy to be bringing on board the former Redress  
15    Officer of the Terrorist Screening Center, who will  
16    certainly be helping us to conduct impact assessments  
17    that may involve the back end nomination process down  
18    the road.

19            It is something that we've seen in other  
20    contexts lately. In reviewing intelligence products,  
21    we see products that are derived from the nomination  
22    process, essentially. So we have built up some subject

1 matter expertise in that area and I think that down the  
2 road that's an area that we'll be examining, too.

3 CHAIRMAN PURCELL: Thank you.

4 I'll call on Joe first, please.

5 MR. ALHADEFF: I think some of these  
6 questions are not necessarily geared on the civil  
7 liberties issue related to this, but I think what ends  
8 up happening is they implicate civil liberties because  
9 of what might be an impression of the program as a  
10 whole, which then leads to a belief that it has a civil  
11 liberties component to it as well.

12 I think, for instance, the notice to  
13 passengers is nice, but at that point it's a little  
14 late to be giving someone notice. That's a notice of  
15 your right to complain. It's not a notice in advance  
16 that this might happen to you, because one might decide  
17 that there are certain personal items that one will not  
18 take on a laptop at a border then, and that should be a  
19 choice that you have. The unfortunate thing is,  
20 terrorists are probably fairly aware of what happens at  
21 a border; citizens are probably much less aware.

22 The concern I also have is how other

1 governments perceive the action of the United States  
2 and then creating a right in them to view the  
3 possessions of Americans as they cross their borders.

4 I know that's not part of what would happen in a  
5 normal PIA, but that has to be a consideration, because  
6 we saw with fingerprinting that some countries  
7 installed fingerprinting where there wasn't a rational  
8 use for them, as there is in the United States, but it  
9 was merely a retaliatory action against an action of  
10 the United States.

11           So I think we have to take a look at these  
12 things as a larger whole, because I think there are  
13 also American civil liberties abroad issues which will  
14 be taken into account by how this works, because in  
15 other countries there may not be as scrupulous  
16 attention to, there was a Privacy Impact Assessment, a  
17 civil liberties review, but rather there have been long  
18 histories of commercial espionage and other reasons for  
19 which people access electronic devices of people that  
20 are traveling. That's not the case of why it's being  
21 accessed in the United States, but that may well be  
22 used as a similar justification for access in a foreign

1 country.

2           So I think, looking at the larger traveler  
3 ecosystem and the broader range of civil liberties  
4 effects, not just on the incoming but also on the  
5 outbound, is an important component. I think notice so  
6 that people are perhaps more aware, because I can see  
7 an American citizen crossing the border having their  
8 laptop searched becoming irate because they had no idea  
9 this was possible, because they don't in their mind  
10 equate the right to search a container with the right  
11 to search a laptop per se.

12           So I think on the civil liberties aspect, I  
13 think you guys have done a fairly good job. I think  
14 the guidelines are fairly well geared toward making  
15 sure there is no targeting done. I think in the  
16 guidance to the officers and the training of the  
17 officers, the behavior of the officer is going to be  
18 critical in this situation, because an attempt to  
19 appear as if they are exerting power is going to be  
20 taken perhaps as, I've been selected for the wrong  
21 reason.

22           Then the last thing I would say is, the

1 concept of having a local escalation for something like  
2 this, so that you don't have to necessarily go to a  
3 complaint that's remote, because by that time that's  
4 when the person thinking of -- it allows the person to  
5 fester, where there could be a way with a local  
6 escalation, especially in larger airports, where that  
7 might be possible, so that you can speak with someone  
8 in a more supervisory role.

9 I think, especially where people suspect that  
10 they have been targeted, speaking to someone in a role  
11 of greater authority may make them feel more  
12 comfortable with what's going to go on and less likely  
13 to have something fester over time which could lead to  
14 a much more difficult complaint to resolve.

15 MR. GERSTEN: I thank you very much for this  
16 input. Certainly the first issue you've raised,  
17 notice, advance notice, is something we do expect to  
18 cover in our impact assessment, and we do expect to  
19 make recommendations related to future notice, perhaps  
20 at the on-boarding, perhaps with a more thorough  
21 campaign of notice just in general to the public.

22 Your second issue is also something that

1 we've looked at, not necessarily in the context of how  
2 to capture that in our impact assessment, but just in  
3 our factfinding. We have discovered that certainly  
4 there are many nations out there that do, of course,  
5 take a look at electronic devices as they go over the  
6 border. Whether or not they are claiming as their  
7 justification for doing so that the U.S. does it, we  
8 haven't seen that yet. But certainly, as you  
9 mentioned, there are other contexts where there is a  
10 sense of retaliation, and certainly it's something for  
11 us to be aware of and look at, not necessarily, as I  
12 say, in the context of our impact assessment, but just  
13 in our general policy discussions in this area.

14 Then the other issue I think is also a very  
15 important one that we'll try to handle in the impact  
16 assessment.

17 CHAIRMAN PURCELL: Thank you.

18 David next.

19 MR. DAVID HOFFMAN: Thank you very much for  
20 coming and talking to us. For those of us that were in  
21 Detroit, we had the opportunity to spend some time with  
22 George, and I think that was very helpful to us, to see

1 the great work that your organization is doing,  
2 particularly reaching out to organizations that are  
3 concerned about civil liberties.

4 One of the things that we observed in Detroit  
5 and heard from Arab Americans in Detroit was a  
6 substantial amount of concern about questions that they  
7 are asked at the border that had to do with the free  
8 exercise of their First Amendment rights, particularly  
9 their right to practice their religion.

10 When we heard testimony or had the  
11 opportunity to talk on the record with someone from CBP  
12 from the office in Detroit, we asked what kind of  
13 guidelines they have to instruct the people, the CBP  
14 agents at the border, on how to avoid asking those  
15 kinds of questions or what questions are prohibited,  
16 and we were told -- and I'm not sure whether this is  
17 accurate or not -- there are no guidelines, that  
18 there's training that's given, but there's no  
19 guidelines and the CBP does not want to restrict in any  
20 way what questions an individual agent could ask  
21 because that would create a security problem because  
22 ultimate freedom would want to be provided.

1           So the committee has requested and is still  
2           waiting for to get more of an answer for that from CBP  
3           on what the training is and whether it's really true,  
4           whether there are no guidelines or not.

5           But this gets to the question I specifically  
6           want to ask you. It wasn't clear to me from your  
7           presentation what the trigger is for doing a civil  
8           liberties impact assessment, because I'm thinking  
9           that's one of the things that could highlight an issue  
10          like that; and then whether that trigger has been  
11          integrated at all with the privacy impact assessment  
12          and the privacy threshold assessment. So is there a  
13          question that could be integrated into the privacy  
14          threshold assessment which would ask, do you ever end  
15          up collecting data in these categories that impacts  
16          civil liberties that then would trigger a civil  
17          liberties impact assessment.

18          MR. GERSTEN: Excellent question. The fact  
19          of the matter is that a civil liberties impact  
20          assessment is not institutionalized to the same extent  
21          that a privacy impact assessment is. There is no  
22          requirement for a program manager to contact our office

1 and tell us that they want us to conduct a threshold  
2 assessment.

3 We have been working on a management  
4 directive, an internal management directive for the  
5 Department, to trigger such an assessment. It has not  
6 been finalized yet. But once that is  
7 institutionalized, the ultimate intention is for our  
8 office to be notified whenever there's a new program or  
9 a major expansion of a program.

10 Now, the scope will be different from a  
11 privacy impact assessment. A privacy impact assessment  
12 may look at a specific computer system or a data-  
13 sharing system, while we may look at a program that has  
14 as part of that program several different data systems.  
15 So really we're talking about two different animals in  
16 some sense.

17 MR. DAVID HOFFMAN: Could I -- well, I would  
18 just offer a comment there and then we can move on.  
19 But I would say I think, while it may seem we're  
20 talking about two completely disconnected and unrelated  
21 animals, I think they are deeply connected. Those of  
22 us who create these kind of impact assessment processes

1 in the private sector oftentimes, while they are  
2 related like that, we put triggers within them. So for  
3 instance, a privacy impact assessment could ask a  
4 question: During the process of this program, will  
5 there be the opportunity to collect or ask questions  
6 about this data element, this data element, religion,  
7 race, ethnicity, which could then trigger.

8 I think there would be a good opportunity  
9 here and I'd recommend exploring with the Privacy  
10 Office whether there's something that could be done  
11 there.

12 MR. GERSTEN: Absolutely. Let me tell you  
13 just briefly --

14 MR. DAVID HOFFMAN: As a multiple trigger,  
15 one of many triggers.

16 MR. GERSTEN: Sure. But let me explain,  
17 there's just a few ways that we have triggered an  
18 impact assessment. Of course I mentioned earlier by  
19 statute; the 9/11 Act asks for four of them to be  
20 conducted. Then of course the appropriations language  
21 required that the Secretary provide a legal framework  
22 and a privacy and civil liberties framework for the

1 National Applications Office and the National  
2 Immigration Information-Sharing Office, and those two  
3 offices -- the certification by the Secretary would  
4 then be approved by GAO, or reviewed by GAO, I should  
5 say.

6 So in both instances, the Department  
7 interpreted that to mean Privacy will conduct a privacy  
8 impact assessment, our office will conduct a civil  
9 liberties impact assessment, and the General Counsel  
10 will provide a legal framework.

11 The other impact assessments have essentially  
12 been triggered by senior leaders. So for instance, our  
13 impact assessment on behavioral protection officers was  
14 triggered when then-head of TSA Kip Hawley met with our  
15 officer and said: We have this new program, we'd like  
16 you to review it. When we reviewed it we said, well,  
17 the best way to actually formalize a review would be to  
18 conduct an impact assessment. That was our very first  
19 proactive impact assessment.

20 Then of course, we've also had program  
21 managers themselves. We've had a program manager  
22 within the Science and Technology component who's come

1 to us with -- or actually briefed -- the senior leaders  
2 of the Department and the chief of staff at the time  
3 asked for our office to take a look at a particular  
4 program that S and T -- a particular research program  
5 at S and T.

6 We sometimes -- because in some instances the  
7 impact assessments are not required by statute, we  
8 sometimes get into a debate with the component about  
9 the scope. So for instance, with S and T are we just  
10 looking at the research itself, the research project,  
11 what the researchers are doing? Perhaps essentially to  
12 give you a picture, it would be tantamount to saying,  
13 are we looking at the laboratory itself or the ultimate  
14 technology?

15 We believe that we need to look at the  
16 ultimate technology. If S&T is going to look at  
17 creating and researching a potential program that could  
18 have widespread ramifications, we need to look at what  
19 ultimately needs to be said to senior leaders in the  
20 Department and DHS partners about that technology. So  
21 there are sometimes scoping issues.

22 We are happy to report that we have finally

1 started to staff our impact assessment work properly.  
2 Up until this year, up until midway through this year,  
3 we actually had not a single person who was full-time  
4 working on impact assessments. Now we have a few that  
5 are full-time and a few that are part-time, and we're  
6 onboarding, as I mentioned earlier, a few more,  
7 including someone who has quite a bit of experience in  
8 redress matters.

9 MS. CALLAHAN: If I could answer the training  
10 question, David -- that David, not this David -- we  
11 discussed the request for follow-up information on  
12 that. We decided to defer that until the training on  
13 the border searches of electronic devices that Civil  
14 Rights and Civil Liberties and Privacy are going to  
15 work on, and have it be as part of that discussion. So  
16 we didn't ignore you.

17 MR. DAVID HOFFMAN: I just think we will  
18 wait.

19 CHAIRMAN PURCELL: Ramon.

20 MR. BARQUIN: Just a quick question. Insofar  
21 as so much of your presentation has focused on the  
22 importance of communicating and clarity in terms of

1 information vis a vis what is happening, whether it's  
2 searches or whatever, I know that as part of our broad  
3 civil liberties environment there has been the  
4 recognition of limited English proficiency citizens and  
5 immigrants. So the question -- I saw nothing at all,  
6 even though I have certainly seen stuff translated into  
7 Spanish or Arabic -- I'm just trying to get a sense of  
8 whether that is something that is within a reasonable  
9 range of priority or whether it's just fallen through  
10 the cracks?

11 MR. GERSTEN: No, it absolutely is part of  
12 our priority. In fact, I'll read the question that we  
13 ask in each of our impact assessments related to  
14 limited English proficiency, if I can find it here.  
15 Essentially, we do ask questions related to Title VI  
16 and limited English proficiency. I think I'm trying to  
17 remember the executive order, 13166, I believe, that  
18 governs federal responsibilities in providing language  
19 access. But we do ask that question quite a bit.

20 Not to say that we are focused primarily on  
21 how a program may disparately impact individuals, we  
22 are essentially looking at intent, not necessarily the

1 strict impact that could be due to many other factors.  
2 But certainly language access is something that we look  
3 at.

4 CHAIRMAN PURCELL: Lisa.

5 MS. SOTTO: Thank you, Richard.

6 David, thank you very much. You have a very  
7 important job.

8 Just piggybacking, really, on David's  
9 question, and I think this is helpful and I think you  
10 answered it in part: Where do you draw the bright line  
11 between privacy and civil liberties, and what falls on  
12 this side of the line?

13 MR. GERSTEN: That's not such a softball,  
14 because I've got Mary Ellen sitting right behind me.

15 MS. CALLAHAN: I know. I'm looking forward  
16 to the answer.

17 (Laughter.)

18 MR. GERSTEN: Well, it's certainly not my  
19 office. Our office does require a political appointee.  
20 We do not have one at this time. I am the acting  
21 deputy. Steve Shih is the acting officer. That  
22 said, historically we have drawn the line based on a

1 number of different factors. I'll give you the dirty  
2 part first. The dirty part is that there are times  
3 when there's not an easy distinction, and really what  
4 matters is which office has better subject matter experts in a  
5 certain area and which office has more resources to  
6 apply.

7           So for instance, on cyber security -- I'll  
8 throw this out here because Privacy, I noticed, has one  
9 of their subject matter experts here on cyber security  
10 -- our office has not really had the personnel to focus  
11 on cyber security until just recently, even though  
12 there are some civil liberties implications. So we  
13 rely on the Privacy Office subject matter expert to  
14 keep us informed as much as possible.

15           That said, certainly after you consider  
16 whether or not a program or a data environment that can  
17 come into play, even after information has been deemed  
18 to be protected for privacy, you could have misuse of  
19 that information which infringes on various rights and  
20 liberties outside of the Privacy Act context. So I  
21 think that's essentially where we draw the line, which  
22 is after you consider privacy we pick up the rest.

1           CHAIRMAN PURCELL: Thank you.

2           Mr. Harper.

3           MR. HARPER: We've had interesting  
4 discussions over recent weeks about the institutional  
5 roles that an organization like yours might play, just  
6 like the Privacy Office might play, independent sources  
7 versus inside, various benefits and burdens of being an  
8 insider or an outsider. Frankly, I'm curious to see,  
9 maybe you could send PDFs or something to be  
10 distributed from the tear sheets, the information that  
11 you sent around.

12           MS. CALLAHAN: It's attached to the back of  
13 the Privacy Impact Assessment.

14           MR. HARPER: Okay.

15           CHAIRMAN PURCELL: Turn around, would you.

16           (Laughter.)

17           MR. HARPER: Because it's very easy for an  
18 organization to potentially mislead people about their  
19 rights. I notice here, and I think you're fairly and  
20 correctly reciting the consensus view on things, but in  
21 your page on border search authority it says: "Border  
22 search authority predates ratification of the U.S.

1 Constitution." And that's certainly factually correct,  
2 but the Fourth Amendment eclipsed any preexisting  
3 border search authority, and the Fourth Amendment  
4 doesn't have any exceptions for borders. It merely  
5 requires reasonableness.

6 Now, case law, through no fault of yours  
7 unless you're a Supreme Court justice I don't know  
8 about, case law has fallen into the habit of saying  
9 that, because so many things are reasonable at the  
10 border, people have a low expectation of privacy,  
11 government's got a high interest in doing all the  
12 things you list here, that they've fallen into the  
13 habit of saying there's no Fourth Amendment rights at  
14 the border. But in fact there are. There's still the  
15 existing requirement of reasonableness.

16 Two pages later you say: "Technological  
17 advances may raise new and unanticipated civil  
18 liberties concerns." I think you could be more  
19 forceful. They do raise. And in your external and  
20 internal communications you could probably be more  
21 forceful, not as forceful as I'd like you to be, of  
22 course. You have to be collegial. But the rationale

1 for border search authority in every law that exists is  
2 interdicting people and contraband, and you have to  
3 start -- you have to reexamine reasonableness when the  
4 potential is that you might search all of someone's  
5 correspondence because of the possibility that they're  
6 bringing a bag of mangoes into the country.

7           So there are -- the container analogy is easy  
8 and cute and it's good for the DHS, but it's not an  
9 analogy that holds up. There are big civil liberties  
10 issues here. Again, inside or outside, it's your role  
11 to be an advocate, but a friendly advocate. But I'd be  
12 worried if you, in your materials, you said to the  
13 public, border search authority predates the  
14 Constitution, because the Constitution trumps past  
15 authority and the Constitution remains in force despite  
16 all statutes and despite the millions of people that  
17 cross the borders.

18           MR. GERSTEN: I really appreciate your input  
19 and I certainly didn't mean to create the impression  
20 that we aren't going to also look at other statutes and  
21 the case law. This is a moving target in some  
22 instances. There are cases being litigated right now

1 involving reasonableness, for instance, of whether or  
2 not if you take the electronic media inside the  
3 country, does that mean that you have seized it at the  
4 border and it applies to the authorities at the border?

5 I think that's United States versus Cotter. So there  
6 are some cases out there right now that we're aware of  
7 and that we're going to make sure that the Secretary  
8 receives our input in our impact assessment, and also  
9 our General Counsel is responsible for taking a look at  
10 the legality and also has an opportunity to perform.

11 MR. HARPER: The other aspect of  
12 reasonableness to consider is that you're not  
13 effectively interdicting the movement of information  
14 into the country by stopping it at the border, as  
15 obviously we have a huge amount of data which is  
16 traveling. So anybody smart enough to know about the  
17 border will just get it into the country some way. All  
18 this goes to the reasonableness, which still applies.

19 CHAIRMAN PURCELL: Thank you.

20 Following a long-held tradition of avoiding  
21 Jim Harper getting the last word, we'll call on Lance  
22 Hoffman.

1 MR. LANCE HOFFMAN: Thank you.

2 Actually, Jim Harper is probably triggering  
3 this comment. I'm noticing a trend -- I want to go off  
4 on something you said, just because I don't know if you  
5 heard the earlier part of it in the morning, where I  
6 and some other people were saying there seems to be a  
7 movement toward legalistic interpretations which are  
8 absolutely defensible legally, but may not go to the  
9 issue of perception and therefore may go to the  
10 ultimate effectiveness of one of these programs.

11 Specifically on the container issue, I think  
12 it's so important to not just say here are the  
13 authorities, here's this, here's that, which I don't  
14 argue with any of it. But somehow it's going to go  
15 past the law to people, and I think it may in the long  
16 run be less effective than at least more explicitly  
17 trying to address those issues he raised, the  
18 rationales. I'll stop there.

19 MR. GERSTEN: I appreciate that input. We of  
20 course have to have a legal analysis in our approach.  
21 That's why we work with our General Counsel's Office so  
22 closely on these impact assessments. However, they are primarily

1 in an effort to examine what you say, what the policy  
2 implications are. We're not paid just to say this is  
3 what they are allowed to do. We're there to say this  
4 is what the impact will be, regardless of the law. You  
5 can have laws that are in place that essentially allow  
6 for your liberties to be taken away. Any time you're  
7 arrested, you're not having liberty, at least for a  
8 short while, and maybe much longer if you've committed  
9 an infringement.

10 So just having a law that says the government  
11 can do something does not necessarily mean that that is  
12 in and of itself a protection. So I fully understand  
13 your comment.

14 CHAIRMAN PURCELL: Thank you, Mr. Gersten.  
15 We appreciate your time today.

16 Now, sadly, we have not received any sign-ups  
17 for public comments. We're beginning to expect that  
18 we're less well loved than we had thought and, happily,  
19 perhaps a little less reviled as well.

20 So I wanted to thank everybody for your  
21 attention today. Members, thank you very much for your  
22 time and your attention, and we'll hereby conclude this

1 public session of the committee. Thank you.

2 (Whereupon, at 11:59 a.m., the meeting was  
3 adjourned.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22