

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

DEPARTMENT OF HOMELAND SECURITY  
Data Privacy and Integrity Advisory Committee

Arlington, Virginia

Thursday, February 26, 2009



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

A T T E N D A N C E

Members (continued):

Lisa J. Sotto

1 PROCEEDINGS

2 MR. BEALES: Good morning, everybody, and  
3 welcome to the public meeting of the Data Privacy and  
4 Integrity Advisory Committee.

5 If -- there's just a couple of housekeeping  
6 items as we get started. If you could please make  
7 sure your cell phones are turned off. We will have  
8 the ring-tone competition at lunch, and you wouldn't  
9 want to give away your secrets.

10 There is, as we noted in the Federal  
11 Register notice announcing this meeting, there's time  
12 for public comments; from 3:30 to 4:00 is what we are  
13 scheduled for. We will probably be adjourning early,  
14 so comments will probably be earlier than that. But  
15 if you would like the opportunity to say a few words  
16 to the committee, we would love to hear from you. But  
17 you need to sign up at the table that's out in front,  
18 and that will be somewhere in the range of 3 o'clock  
19 or something like that.

20 We begin today by hearing from the -- from  
21 John Kropf, the Acting Chief Privacy Officer. John  
22 became the Acting Chief Privacy Officer on January

1 21st. I wonder why that particular day. He first  
2 joined the Privacy Office in 2005 as the Director of  
3 International Privacy Policy, and he's also served as  
4 the Deputy Chief Privacy Officer.

5 So, welcome, John, and we look forward to  
6 hearing what's happening in the office.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 DHS PRIVACY OFFICE UPDATE

2 MR. KROPF: Thank you very much, Mr.

3 Chairman, and vice chair, and to the rest of the  
4 committee. I would simply like to start by thanking  
5 you for your continued service to the Department and  
6 your continued service to this country, because you  
7 are providing a very, very valuable resource and a  
8 very valuable source of advice for the Department of  
9 Homeland Security.

10 What I would like to do this morning is  
11 update you on the activities of the Privacy Office  
12 since the committee's last meeting, December 3 of  
13 2008. The committee is going to hear presentations  
14 this morning after my summary. They'll hear  
15 presentations this morning and in the afternoon on the  
16 Office's extensive international activities, our FOIA  
17 and disclosure program, and particularly on traveler  
18 redress in the afternoon. And then, of course,  
19 following that we will have reports from the  
20 subcommittees, and we're very much looking forward to  
21 what the subcommittees have to report out.

22 So there's some general items and there's some

1 specific that I would like to take you through as we  
2 review the activities of the Office. First off, this  
3 is a very exciting time for privacy and for the  
4 Privacy Office. We are at a moment of transition in  
5 many ways. Many privacy standards are still being  
6 worked out and devised, and this is a very exciting  
7 time for anybody who is a privacy professional. And  
8 for the Office itself, we're extremely excited for a  
9 number of reasons in particular.

10 I think it almost goes without saying, but  
11 first and foremost we are absolutely delighted that we  
12 have now a new Chief Privacy Officer named Mary  
13 Ellen Callahan, who is a very, very experienced  
14 privacy expert from the law firm of Hogan and Hartson,  
15 where she is a partner there, and also serves as the  
16 co-chair of Online Privacy Alliance and the vice chair  
17 of the American Bar Association's Privacy and  
18 Information Security Committee, which is part of the  
19 anti-trust division. So we are absolutely looking  
20 forward to working with her and supporting her vision  
21 for the Office. I think I have to say that probably  
22 no one is more excited than the acting Chief Privacy

1 Officer to have this appointment.

2 I also would note that I think an  
3 appointment so early on in the transition is a sign  
4 that the Privacy Office is well established in the  
5 mind of the Secretary for the Department, that we're  
6 thought of so early in the transition.

7 The other reason I think to be excited is  
8 that the first full day of the new administration  
9 coming on board on January 21, there are two White  
10 House memos that were issued that are of great  
11 significance to the mission of the DHS Privacy Office  
12 in particular.

13 The first of those memos detailed a more  
14 robust, more forward-leaning approach to Freedom of  
15 Information Act disclosures and processing, and the  
16 Freedom of Information Act is something that we'll  
17 hear about later during the day, but it is certainly  
18 among the core responsibilities of the DHS Privacy  
19 Office, and this we think also bodes well for the work  
20 of the Office.

21 The second White House memo that came out  
22 had to do with transparency and really trying to use

1 technology and try to be as forward-leaning as  
2 possible in informing citizens and individuals of what  
3 the government is up to. And again, this is --  
4 transparency is a concept fundamental to what we do in  
5 the Privacy Office. It is the basis of the trust that  
6 we create with the public for the activities of the  
7 Department of Homeland Security.

8           Transparency really underlies, again, a lot  
9 of the compliance that we do. It underlies the System  
10 of Records Notices. It underlies the Privacy Impact  
11 Assessments. So those two memoranda I think will  
12 support us well as we move forward in our mission with  
13 the Office.

14           And then the other general comment I'd like  
15 to note is we note the committee's letter to the  
16 Secretary, which she has received and personally noted  
17 and replied back to the Privacy Office that she is  
18 commending this letter to the attention of the new  
19 incoming Chief Privacy Officer. So we note your  
20 letter and the 16 recommendations and look forward to  
21 responding to them.

22           Now I'd like to go from the general to the

1 specific and just take a bit of a tour through each  
2 one of the sections and functions of the Office and  
3 give you some updates.

4 Starting with the compliance area, there's  
5 a bit of an overlap from our last meeting, but I  
6 really want to focus on this particular effort that we  
7 had ongoing at the time, which is the Legacy System of  
8 Records Notice Project, which was completed after 14  
9 months of effort. This is essentially taking all of  
10 the Legacy Systems of Records Notices that were --  
11 came from the 22 different pieces of agencies that  
12 were consolidated to help form DHS, and this involved  
13 a review of 213 Legacy SORNs.

14 The Department's final inventory of this  
15 review now includes 130 SORNs. Many of these older  
16 SORNs could be retired or consolidated. This is  
17 significant because it is probably the largest privacy  
18 compliance effort that's been conducted by any single  
19 agency I think since the history of the Privacy Act,  
20 and it's no small achievement. It's an extraordinary  
21 achievement to be noted for our compliance team.  
22 Everybody did a fantastic job concluding that project.

1           Other activities in the compliance area  
2 include what we have underway right now, which is a  
3 review of all the Notices of Proposed Rulemakings  
4 under the Privacy Act. These are the exceptions that  
5 have been proposed for particular systems of records  
6 notices, and we're reviewing all the public comments  
7 that have been received, and our goal is to make all  
8 of these proposed rules into final rules after  
9 reviewing the public comments.

10           Another activity that's underway is to  
11 establish a timetable for a biannual system of records  
12 notice review. The SORNs that were not reviewed as  
13 part of the Legacy SORN Project are projected to be  
14 reviewed before September of 2009, and then after that  
15 we plan to set a schedule to do a biannual review of  
16 all SORNs for the Department after that.

17           In the policy area, January was a very  
18 active month for us. We're extremely -- I want to say  
19 proud to have put out two privacy policy memoranda.  
20 The first is the memoranda that enshrines the Fair  
21 Information Practice Principles as the core principles  
22 of the Department of Homeland Security's privacy

1 principles. It is -- it is, I think, a unique  
2 statement in at least one area of the FIPPs. We're  
3 very forward leaning on the area of data minimization,  
4 and we're pleased that that was issued.

5 The other privacy policy that was issued  
6 was a Privacy Office guidance on standards for  
7 conducting PIAs, or Privacy Impact Assessments, for  
8 DHS technology programs and information collection.

9 And then an upcoming event in the policy  
10 area which I'd like to note is that senior privacy  
11 staff will be conducting outreach at the National  
12 Fusion Center conference in March in Kansas City. We  
13 have a number of our senior staff going to participate  
14 on a panel at this conference, a learning lab, and  
15 they are going with CRCL to also man a booth at the  
16 conference to further their outreach activities.

17 Turning just for a moment now to the  
18 privacy technology and intelligence area, we continue  
19 to work with the chief information officer to develop  
20 an approach to privacy compliance for service-oriented  
21 architecture, and on this particular point we're  
22 looking forward to the subcommittee -- benefiting from

1 the committee's guidance in this area. We understand  
2 that there's been subcommittee work that's  
3 forthcoming.

4 We're also working with the Science and  
5 Technology Directorate to develop an implementation plan  
6 for the privacy principles that came out of our data  
7 mining report from 2008, and we continue to hold a  
8 leadership role in the area of biometrics. We serve  
9 on the DHS Biometrics Coordination Group, as well as a  
10 White House National Science and Technology  
11 Subcommittee on Biometrics and Identity Management.

12 FOIA is the next area, and as I mentioned,  
13 we'll have a presentation later today on the details  
14 of the FOIA program by our Associate Director, Bill  
15 Holzerland. But I just wanted to briefly mention to  
16 you a couple of areas of significance.

17 We've had our 2008 FOIA annual report  
18 issued last month to the Attorney General, and this is  
19 the first -- the significance of this report, it's the  
20 first report to implement the requirements of the Open  
21 Government Act of 2007.

22 We've also hired three additional FOIA

1 specialists to handle further reductions in our  
2 backlog.

3           With a new area now, I'd like to mention  
4 Privacy Incidents and Inquiries. We have -- we have  
5 still a relatively new Director for Privacy Incidents  
6 and Inquiries with the Privacy Office. She has now  
7 gone to meet a number of the -- the major components  
8 within DHS, to craft an incident response team at the  
9 component level, and to really foster some trust and  
10 collaboration with those components. At the same  
11 time, she's working on developing an electronic  
12 complaint tracking system to address privacy  
13 complaints and respond to access requests and provide  
14 redress as appropriate. This will also help us with  
15 our Section 803 quarterly reporting requirements to  
16 Congress.

17           Now I'm going to turn to our international  
18 privacy policy team. You will be hearing a brief, I  
19 believe, following my presentation here from Shannon  
20 Ballard and Lauren Saadat, who are Associate Directors  
21 and will provide you with a comprehensive review of  
22 our international work. It is actually quite a

1 significant area for the Office.

2 I will mention briefly a couple of things  
3 that they may not cover. First is in January, I  
4 believe it was January 12, we sent a representative to  
5 Barcelona to attend as observers the Spanish Data  
6 Protection Authority's meeting that they hosted in  
7 collaboration with the Catalan data protection  
8 authority's discussion of global privacy standards;  
9 and DHS, together with FTC, were invited to come to  
10 this meeting, to sit in as observers.

11 This is an initiative that was created  
12 following the 2008 Strasbourg Conference of  
13 International Data Protection Commissioners. And the  
14 initiative is to really -- really is based on a  
15 resolution that was passed in Strasbourg to call upon  
16 the United Nations to create a binding international  
17 set of privacy standards.

18 And what the Spanish hope to do from that  
19 resolution is craft a document that would be reviewed  
20 and presented at the 2009 conference which they are  
21 hosting in Madrid, and this document would then be  
22 passed on in theory to the United Nations to review

1 and possibly act upon.

2           It's something that, just in terms of our  
3 observations at that meeting, there were a total of 40  
4 full members of the International Data Protection  
5 Conference that were there. Of those members, they  
6 were entirely made up of European representatives,  
7 plus a Canadian contingent, and then there were 27  
8 experts who attended representing industry, legal  
9 community and academics, as well as NGOs, and then FTC  
10 and ourselves.

11           The interesting thing to note for the scope  
12 of this project is it is very wide-ranging. The body  
13 is really asking that they create standards not just  
14 for the commercial world but also for law enforcement  
15 and other government activities. So it would be a  
16 full scope document, a full scope of standards for all  
17 activities that involve the use of personally  
18 identifiable information.

19           One of our observations also from this  
20 meeting is much of the conversation really focused on  
21 the European -- the Council of Europe Convention 108  
22 and the 1995 Directive from the European Union. They

1 expect to hold two more meetings before the Madrid  
2 Conference in November, and we are standing by to see  
3 if we continue to be invited as observers. As  
4 observers, we do not have the opportunity to actively  
5 participate, but we were able to simply note that it  
6 seems as if they have a very ambitious plan ahead of  
7 them, given the scope of their designs.

8           The other thing -- the other two items I'll  
9 mention under the international are in January we  
10 issued an interim report on the European Union's  
11 approach to commercial collection of personal data for  
12 security purposes, and this largely focused on the  
13 European hotels' practice of collecting personal  
14 information. And Lauren Saadat will, in her  
15 presentation later, go into some detail about this  
16 particular report.

17           I'd also like to mention that last month  
18 our Associate Director, Shannon Ballard, was invited  
19 to Mexico to brief members of the Mexican Senate on  
20 the U.S. privacy framework with respect to how the  
21 government handles and maintains personal information.  
22 This was, I believe, a full collection of senators who

1 were interested to hear how we have devised the  
2 Privacy Act and implemented the Privacy Act since  
3 1974. This complements an earlier presentation they  
4 received from the European Union representatives.

5 That is really a quick snapshot of what we  
6 have been up to since December, and as far as the  
7 future goes, there are many, many issues that we have  
8 on our plate, and many that are underway. I could  
9 single out a few, such as I think for future activity  
10 that we expect to see more work in would be cyber  
11 security and social networking, and there are many  
12 others as well. Information sharing continues to be a  
13 big one.

14 But the Office certainly has a lot ahead of  
15 it, and we're looking forward to digging in and  
16 continuing our work.

17 I'd also just like to pause here for a  
18 moment, and to turn and thank Martha Landesberg, who  
19 is the Designated Federal Official for -- this is her  
20 first meeting to organize, and I think she's done an  
21 outstanding job, and I would just like to commend her  
22 for her hard work in putting this together.

1           So with that, I'm going to stop and take  
2 any questions that you might have. Thank you.

3           MR. BEALES: John Sabo.

4           MR. SABO: Thank you, John. A quick  
5 question. You know, you participated in Barcelona as  
6 an observer, and I guess the question goes to what  
7 level of treatment does -- and, in effect, you and the  
8 FTC were representing your agencies, I presume, and  
9 not the U.S. Government. But to what degree are you  
10 given equal treatment with respect to decision-making,  
11 as opposed to merely being observers, and to what  
12 degree is the lack of a Federal privacy officer a  
13 detriment to engaging with international data  
14 protection commissioners and the communities?

15           It's not asking a political question. It's  
16 asking a -- basically an operational question as to  
17 how much influence can you have if you're basically an  
18 observer versus an active participant?

19           MR. KROPF: Well, I'm not sure if -- just  
20 to understand the question a little bit more, is it if  
21 we could have a single representative for the United  
22 States Government to speak on behalf of privacy?

1           MR. SABO:  It's really more to our -- for  
2           example, you've done other international engagements  
3           with data protection communities.  So the question is  
4           are you given -- because of the importance of this  
5           privacy office, are you given equal treatment with the  
6           other national representatives?  For example, Spain or  
7           Germany and so on, in terms of the debate and the  
8           decision-making and voting and so on?

9           MR. KROPF:  This particular body, the  
10          International Conference of Data Protection and  
11          Privacy Commissioners, has specific criteria for full  
12          membership, and those criteria track largely European  
13          notions of adequacy, and among those criteria is one  
14          that a data protection authority must be independent  
15          from the government, and that is really more  
16          particular to the European government structure.

17                 It's not something that I'm not -- it's not  
18          something I'm sure we could meet that criterion if we  
19          wanted to.  So I think when we did apply for full  
20          membership status some years ago, the failure to meet  
21          that particular independence criterion was looked at,  
22          and I think the compromise was, well, we would be

1 given observer status. As observers, we generally --  
2 we have no voice in the debate. We have no  
3 opportunity to vote. We certainly can try to make our  
4 views known on the margins, but we are limited in what  
5 we can do in this capacity. Does that get to what you  
6 were asking? Okay.

7 I see other cards are up. Should we just  
8 go to the --

9 MR. BEALES: Sure. Lisa Sotto.

10 MS. SOTTO: Thank you. John, thank you so  
11 much for your leadership over the last month or so.  
12 Really -- really tremendous leadership. Thank you  
13 from, I think, all of the committee.

14 I want to commend the Office particularly  
15 for developing the FIPPs. I think that's a very  
16 important document and will serve you very well going  
17 forward. I particularly like -- obviously, it's quite  
18 reminiscent of some documents that are already out  
19 there, particularly APEC. But I particularly like  
20 some of the deviation from APEC, which was carefully  
21 considered, I'm sure.

22 So my question really is how do you

1 anticipate using these principles going forward? Are  
2 they aspirational? Do you have more concrete uses in  
3 mind rather than just an aspirational baseline?

4 MR. KROPF: Well, thank you for the kind  
5 words, and I think that really the driving force here,  
6 I have to give a lot of recognition to our Director of  
7 Policy and Senior Advisor, Toby Levin, who really  
8 shepherded this statement of the FIPPs through, and if  
9 there's an opportunity for her to speak, I'd also like  
10 her to give her two cents.

11 But I see this articulation of the FIPPs as  
12 really a foundation from which we can build our  
13 Privacy Impact Assessments, from which we can do  
14 refinement, perhaps, of our other privacy compliance  
15 requirements, Systems of Records Notices and so on.

16 I'm looking to Toby. If -- with the  
17 committee's indulgence, we can have her come to the  
18 microphone. For the court reporter, this is Toby  
19 Levin, who is our Director of Policy.

20 MS. LEVIN: I very much appreciate John's  
21 remarks, and yours as well, Lisa.

22 I think I wanted to share with you that

1 this articulation really is not the beginning but the  
2 -- it captures actually the principles that we have  
3 sought to implement for the last, certainly the last  
4 year and a half specifically through our Privacy  
5 Impact Assessment analysis, through the PIAs that  
6 we've issued within a number of significant  
7 rulemakings.

8           If you look back at those PIAs regarding  
9 Real ID and WHTI and state and local fusion centers,  
10 you'll see that they follow the FIPPs analysis, the  
11 principles that we discuss in this memorandum. So to  
12 Chief Privacy Officer Hugo Teufel's credit, he felt  
13 that it would be very helpful to have this  
14 articulation as a memorandum for the Department, but  
15 it really captures what we have been doing day in and  
16 day out.

17           In our meetings with component programs,  
18 when they ask, "Well, what do you mean when you say we  
19 want you to consider privacy and mitigate privacy  
20 concerns," what we do is we walk them basically  
21 through these FIPPs principles.

22           So they are certainly always aspirational

1 but absolutely part of our daily operation, and we  
2 appreciate your thoughts individually or collectively  
3 on the principles. But they absolutely guide  
4 everything we do.

5 MR. BEALES: Ana Anton?

6 DR. ANTON: So, Mr. Kropf, thank you very  
7 much for your tremendous leadership and work, and  
8 active leadership during this time, and we appreciate  
9 all your efforts.

10 You mentioned that two up and coming or two  
11 things that are coming up on the radar are cyber  
12 security and social networking, and I was wondering if  
13 you might be able to elaborate a bit on that, and in  
14 particular what the role of -- what you view as the  
15 role of DHS, the DHS Privacy Officer and Office with  
16 regard to these two areas, or if you meant them as  
17 one.

18 MR. KROPF: I mean, just to speak very  
19 generally, information is the lifeblood of DHS, and  
20 wherever information is involved, personal information  
21 is involved, and so the Privacy Office is going to be  
22 right there. And when you're talking about cyber

1 security, personal information is something that will  
2 be part of that effort.

3 In a very broad way, I know there's  
4 currently a 60-day review that's underway led by the  
5 White House in terms of what next steps to do with  
6 cyber security. But we have been very involved up to  
7 the present in ensuring that any PII handled in the  
8 cyber security effort is appropriately protected.

9 We have issued a Privacy Impact Assessment  
10 on the Einstein Program, and we have a very close  
11 relationship with all of the cyber security elements  
12 of DHS through the leadership of Pete Sand and his  
13 team, the Technology and Intelligence team. He is --  
14 I want to say, just at a very practical level, we have  
15 been attending meetings with them regularly so that  
16 we're closely connected to all developments and we can  
17 be there at the creation when a question comes up about  
18 personal information.

19 On social networking, there's simply a  
20 lot of interest in our office in seeing what we can do  
21 to contribute to protecting personal privacy because,  
22 obviously, this is a hot topic and the government is

1 very much interested in using social networking tools.  
2 And as we can see from the White House memoranda about  
3 improving transparency, they really do want to push  
4 these kind of tools, these new technological tools to  
5 increase that transparency. But you are going to have  
6 attention there with how do you protect PII at the  
7 same time.

8 So we're looking for ways to continue our  
9 leadership in the social networking area in terms of  
10 privacy, if that answers your question.

11 Other questions?

12 MR. BEALES: Joanne McNabb.

13 MS. McNABB: Thank you, John, and Toby. I  
14 was -- I rather gathered that the FIPPs document was  
15 presented as a summary, the way you've been  
16 approaching, carrying out your mission;, and I  
17 wondered if you had considered -- had got, in  
18 developing that document and sort of looking at how  
19 you approach privacy, if you had gone back to look at  
20 the framework document that this committee provided  
21 several years ago, which actually starts a step  
22 earlier.

1           FIPPs starts with you've got the data; how  
2 do you manage it responsibly. The earlier step in the  
3 framework is should you, for this purpose -- is this  
4 the way to accomplish this purpose, which would lead  
5 you to ask, in some cases, should we be getting the  
6 data at all.

7           MR. KROPF: I think absolutely, we did go  
8 back and look at the earlier work of the Committee.  
9 I'm going to give Toby an in here if she wants, but I  
10 think your question also goes to the very first  
11 question you ask of any program is, do you have the  
12 lawful authority to collect this information in the  
13 first place, and that's always the starting point. Is  
14 that --

15           MS. McNABB: No, even a little before that.

16           MR. KROPF: Even before that?

17           MS. McNABB: Does this program, which is  
18 going to collect personal information presumably, does  
19 this program, is it designed -- is it the best way to  
20 meet the objective?

21           MR. KROPF: Toby, I'm going to ask you to  
22 sit in on this, since you really were the drafter.

1 But I want to take another comment here and ask if  
2 it's also closely related to data minimization, do you  
3 need the data at all, in the first place.

4 MS. McNABB: Certainly, certainly.

5 MR. KROPF: And if you do need it, what are  
6 the least number of data elements that you could use  
7 to accomplish the mission?

8 MS. McNABB: It's even before that. I  
9 mean, certainly that's a piece of it. It's the  
10 efficacy of the program at all.

11 MS. LEVIN: I think certainly the point you  
12 raise is clearly embedded within the analysis.  
13 Remember, we -- the PIA is a process. It is a tool  
14 which we use to help programs do decision-making  
15 about their activities and how to address privacy.

16 So the document itself is -- doesn't  
17 reflect the discussion and the dialogue that occurs  
18 around it. So the very point you make is when  
19 programs describe their objectives to us, that  
20 question about alternatives and approaches is part of  
21 that discussion. The actual template that we use may  
22 not reflect all of that discussion that occurs around

1 the document or in terms of the principles.

2 We didn't spell that out specifically,  
3 although you may have seen in our workshop report on  
4 data mining, we did develop a set of research  
5 principles with our Science and Technology  
6 Directorate, and those specifically, there is a  
7 reference to an analysis of efficacy as part of that  
8 research discussion regarding the FIPPs.

9 So if you're suggesting it might be good to  
10 actually pull out and have a specific principle with  
11 regard to efficacy, that's something we can certainly  
12 consider. But I want to assure you that discussion  
13 occurs because we do ask for them to describe why they  
14 think or how they think this will work and how  
15 effective it will be, and to the extent that there's  
16 data that they can share with us, that they have data  
17 to share, that is part of the discussion. But I  
18 appreciate what you're saying in terms of it not being  
19 separated out.

20 MS. McNABB: I think it would be a good -  
21 it would be, I think, interesting to know if it's  
22 useful to the Department, to the Office, to begin the

1 discussion at that level, rather than --

2 MS. LEVIN: But recognize how awkward it  
3 can be for the Privacy Office to question a component  
4 about whether or not they think this is an effective  
5 program. It's done within the context of tell us how  
6 you're proposing to do it, and as John said, the data  
7 minimization principle and how do you intend to use  
8 the information. And through that discussion, I think  
9 we do have an opportunity to understand the basis on  
10 which they're making those decisions.

11 But obviously, the component heads and the  
12 Secretary ultimately make the decision about whether a  
13 program is effective or not, and privacy is just a  
14 part of that.

15 MS. McNABB: And a big part. You're up to  
16 it.

17 MR. KROPF: And I would just add if, after  
18 reviewing our statement of the FIPPs, if the Committee  
19 would like to offer some advice on that, we're happy,  
20 of course, to hear it.

21 Other questions?

22 [No response.]

1           MR. BEALES: Well, John, thank you very  
2 much for being with us. I want to -- and I know  
3 transitions are challenging times, and I want to  
4 congratulate you on the leadership you've shown in the  
5 Privacy Office and in getting through to the next  
6 administration. But I think the whole Committee  
7 really appreciates it.

8           MR. KROPF: Thank you very much, and I'm  
9 looking forward to working with you in the future, at  
10 future meetings, and having our new CPO up here for  
11 the next one. Thank you.

12          MR. BEALES: Thanks.

13                 Next on our agenda is an update on the  
14 Privacy Office's international activities. We have  
15 with us Shannon Ballard and Lauren Saadat, who are  
16 both Associate Directors for International Privacy  
17 Policy. They are responsible for policy development,  
18 for advising senior leadership on international  
19 privacy law and policies, and for monitoring DHS  
20 security activities for their impact on international  
21 privacy issues. They represent DHS at meetings of  
22 multilateral and multinational organizations,

1 including APEC and OECD, and they engage in bilateral  
2 dialogues with representatives of foreign governments  
3 and data protection authorities.

4 So welcome, Ms. Ballard, Ms. Saadat. We  
5 look forward to hearing from you.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 DHS PRIVACY OFFICE INTERNATIONAL ACTIVITIES UPDATE

2 MS. BALLARD: Good morning. Thank you, Mr.  
3 Chairman, vice chairman, committee members. This is a  
4 real honor for Lauren and me. This is our first time  
5 to address the Committee, so we certainly appreciate  
6 this opportunity to explain to you a little bit about  
7 what we do internationally for the Office, and we look  
8 forward very much to your feedback and your input on  
9 our programs and what we do here.

10 As a team, as always, Lauren and I, what  
11 we're going to do this morning is we're going to split  
12 the presentation. I'm going to go over a little bit,  
13 give you an overview of our international activities,  
14 what we do internationally and why it's important, and  
15 touch on a few of the major activities, similar --  
16 going a little bit further than what John did this  
17 morning. And then Lauren will take over and discuss a  
18 little bit more in depth about what lies ahead, what  
19 we see as important areas, and to seek your feedback  
20 on certain policies and programs.

21 You should have a PowerPoint presentation,  
22 if you want to -- if you're interested in following

1 along on the paper or up ahead.

2           So why does privacy have -- the Privacy  
3 Office have an international mission? As you know  
4 here, in the private sector and NGOs and educators,  
5 information flows are global, and that goes the same  
6 for DHS and the public sector. So we work  
7 internationally and within the Department to  
8 positively influence international discussions that  
9 concern privacy and security protection in a homeland  
10 security context.

11           Our primary goal is to promote  
12 international cooperation and understanding of privacy  
13 issues relevant to the Department's mission and our  
14 operations. To do this, we enhance information-  
15 sharing opportunities with our international partners  
16 by providing educational outreach and leadership in  
17 areas such as PIAs and the Freedom of Information Act.

18           We also develop and integrate DHS-wide  
19 guidance on privacy requirements for international  
20 information-sharing agreements. Similar to what we  
21 just discussed with the FIPPs, we take that another  
22 step and look at it when we have international

1 agreements bilaterally and multilaterally with the  
2 Department.

3 We interpret or try to interpret  
4 international data protection frameworks. We look at  
5 what's reported in the press through personal  
6 relationships that we have. We monitor new  
7 developments and changes in legislation that may  
8 impact our information-sharing opportunities.

9 We counsel DHS and other departments within  
10 the United States Government on existing and emerging  
11 changes in privacy practices and policy approaches and  
12 how we see it impacting our mission.

13 We meet and talk with international privacy  
14 commissions and bilateral partners, as well as engage  
15 in multilateral forums such as OECD, APEC, the  
16 commissioners conference John had mentioned, and also  
17 a big one for us most recently is the ISO, the  
18 International Organization for Standardization.

19 We provide counsel and expertise on  
20 international agreements related to PII collection and  
21 sharing that may impact DHS' mission. And finally, we  
22 serve as a point of contact for our international

1 partners.

2           So why should governments share  
3 information? Well, obviously, after the 9/11  
4 Commission Report came out, that was a major thrust  
5 and one that the Privacy Office has taken to heart.  
6 So our leadership has recognized that the trust of our  
7 partners is integral to achieving our mission in the  
8 Department.

9           In 2007, we issued a policy memorandum that  
10 addressed the privacy protections for non-U.S.  
11 persons. Given that the Privacy Act doesn't  
12 necessarily cover non-U.S. persons, the full - the  
13 policy statement gives administrative coverage to  
14 those persons who have information in a mixed-use  
15 system within DHS, and we have used that quite  
16 extensively to increase the trust among our  
17 international partners to show them that although the  
18 Privacy Act doesn't explicitly state as much, DHS has  
19 made a commitment to providing such privacy  
20 protections to non-U.S. persons.

21           And our components are committed to the  
22 fair information principles as set forth in the

1 Privacy Act for non-U.S. persons. And at U.S.  
2 VISIT, we have a representative of our privacy  
3 component officer here today. That's one example of  
4 how a component has taken the FIPPs and put them into  
5 practice, in place, and it's gone pretty far with our  
6 international colleagues that demonstrates how these  
7 privacy principles are put into a program.

8 So next slide. So, another question. Why  
9 is privacy important for DHS international affairs?  
10 Obviously, government programs that have real or  
11 perceived privacy problems can face great scrutiny  
12 here at home, but even more so overseas. So that  
13 negative perception with our international partners  
14 could lead to resistance in sharing the information.

15 More and more often, we're finding that  
16 privacy or data protection is being used as a foreign  
17 relations tool or a political tool. So DHS needs to  
18 demonstrate effective privacy practices and engage the  
19 international community so DHS missions and objectives  
20 are not impeded by lack of understanding on how we do  
21 privacy.

22 And as noted here, there's a few examples

1 of how those perceived privacy problems can  
2 significantly impact DHS programs. And if these  
3 programs don't move forward -- PNR, for example -- we  
4 have -- that could impact our relations in other areas  
5 as well. Again, it goes back to the trust among our  
6 international partners, the effectiveness of the  
7 privacy principles within our programs, and how DHS  
8 meets our objectives to secure the homeland while also  
9 protecting the personal information of the  
10 individuals.

11 So building on the topic of trust in our  
12 international partners, we believe that if our  
13 international partners understand and have confidence  
14 in our privacy practices, then trust is built between  
15 us. DHS cannot look only within itself, or even  
16 within the U.S. Government, to effectively carry out  
17 our mission.

18 So as I mentioned, information flows across  
19 borders more rapidly than ever before. Information  
20 held by one country may be critical for another.  
21 Trust between global partners is imperative. We must  
22 earn this trust and can't simply make demands on other

1 sovereign countries.

2           So understanding each other's history and  
3 culture and taking the time to establish relationships  
4 makes for more effective international discussions,  
5 and hopefully more effective operations. However,  
6 talk alone will not solidify those relationships. We  
7 must demonstrate consistently that -- how we live up  
8 to the claims we make and demonstrate our commitment  
9 to effective privacy protections.

10           And I'm just going to touch on a few  
11 examples of what Lauren and I have been spending our  
12 time on and how international privacy policy is  
13 embedded within policy issues within the Department,  
14 within programs, PNR, the Passenger Name Record  
15 negotiations with the European Union, and other  
16 bilateral and multilateral information-sharing  
17 agreements.

18           The one thing that we believe makes us more  
19 effective is that the Privacy Office is invited to the  
20 negotiating table at the beginning, when these  
21 agreements are coming into place. We sit at the table  
22 and we talk about, well, what information do you need?

1 Do you need that information? How are you going to  
2 use it? How are you going to protect it? So that is  
3 built into the framework, into the agreement at the  
4 beginning, whereas a number of our partners overseas  
5 may not see that agreement until after it's already  
6 been signed. They can use the press and they can use  
7 other means to make waves and possibly make changes to  
8 it. But I think what makes our Office more effective  
9 is that we are actually there and able to get our  
10 points heard and included in those agreements.

11 MS. SAADAT: Just a little footnote to  
12 that. We -- it's a little frightening, but sometimes  
13 our foreign partners, independent data protection  
14 commissioners, only find out about agreements,  
15 information-sharing agreements, with DHS when they  
16 read our Privacy Impact Assessment on our website. So  
17 that goes some way to proving our case that we take  
18 privacy seriously here at the Department.

19 MS. BALLARD: When they don't have a PIA  
20 for their own ministry or that negotiating agreement  
21 with us. So, yeah.

22 So when we are examining and assessing

1 international privacy practices, again, we participate  
2 in a number of multilateral forums. We monitor press  
3 and other discussions and dialogues that take place  
4 not only among privacy commissioners and experts, but  
5 also within the law enforcement and counter-terrorism  
6 community.

7 We have ramped up in the past year an  
8 international exchange program. We've hosted a number  
9 of countries to the Privacy Office for about a week at  
10 a time, and we've given them an in-depth overview of  
11 all the different divisions within the Privacy Office,  
12 explained to them what we do and how we do it. We've  
13 also exposed them to other offices within DHS and the  
14 U.S. Government, particularly when it comes to  
15 oversight.

16 As John mentioned, with the commissioners  
17 conference and our independence, we often have to  
18 explain how we do oversight within the U.S.  
19 Government. It's called the Networked and Layered  
20 Approach, which includes the Inspector General, GAO,  
21 OMB, and others. So we've done well.

22 Lauren and our compliance director went to

1 the U.K. and spent a week in the U.K. Information  
2 Commissioner's office on an exchange program, again to  
3 give us and them more of a time to share best  
4 practices, learn more about how each other -- how we  
5 do privacy.

6 We will -- we have plans to host another  
7 one at the end of April, and we see that as being very  
8 effective to improving communications, relations, and  
9 understanding.

10 Lauren and I will review PIAs and SORNs,  
11 particularly when they have an international element  
12 to them. As John mentioned, I was in Mexico City  
13 earlier this year. Lauren will be traveling to Europe  
14 in about two weeks and participating in a number of  
15 meetings and opportunities to discuss DHS' activities  
16 when it comes to privacy.

17 We coordinate international participation  
18 in DHS events by seeking international experts that  
19 will help to inform DHS programs and policies that  
20 have an international impact.

21 And the last bullet point there about  
22 explaining DHS privacy policies and programs, that has

1 taken up quite a bit of our time, and we spend a lot  
2 of effort, whether we write an article or answer  
3 questions from other privacy commissioners or law  
4 enforcement authorities, trying to dispel the myth and  
5 to demonstrate and show the transparency that we have  
6 within the Department in our Office on how we do  
7 privacy, and explaining to them, showing them what  
8 they can actually look to about what we do when it  
9 comes to protecting information. As John mentioned,  
10 DHS does collect quite a bit of personal information,  
11 and dispelling those myths with the international  
12 community is a huge effort on our part.

13 So I'm going to turn it over to Lauren now  
14 to talk about developments that were things that we  
15 think are important that we're watching and give you a  
16 little bit of insight on some major programs that you  
17 may already be aware of, and also to seek your  
18 feedback. Thank you.

19 MS. SAADAT: So these are really  
20 developments that we're watching and in some cases  
21 participating in, in 2009.

22 John touched briefly already on the

1 international data protection commissioner's call for  
2 a U.N.-based privacy resolution based on Council of  
3 Europe Convention 108. So I think that -- if they are  
4 successful, that can have an impact on DHS programs.

5 We're working -- we are now members of CS1,  
6 which is the U.S. Technical Advisory Group to the  
7 International Standards Organization, because the ISO  
8 is working on an actual -- actually, several -- there  
9 is a privacy standard, and then there are other  
10 standards that also are privacy-related.

11 We are -- we participate in the OECD  
12 Working Party on Information Security and Privacy, and  
13 that's actually one of the reasons why I'm going to be  
14 going to Europe in March. There is a global privacy  
15 dialogue that is occurring in the OECD, that will  
16 culminate in a conference to take place in 2010, which  
17 is the 30th anniversary of the OECD privacy  
18 guidelines. So we'd like to play a role in shaping  
19 that dialogue.

20 We are watching very carefully the  
21 examination of the 95 Directive in Europe. There are  
22 -- well, there were three sort of reviews going on.

1 One is by the Commission, had convened a group of  
2 experts that has very recently been disbanded that  
3 were reviewing the 95 Directive. A second one, the  
4 Information Commissioner of - Commissioner's Office of  
5 the U.K., has commissioned Rand to do a report. That,  
6 I believe, is going to be coming out in April. And  
7 then there's a third one that's taking place that's  
8 mostly just a legal review that's taking place by an  
9 EU body out of -- working out of Vienna.

10 The reason why the 95 Directive is so  
11 interesting to us is that sometimes the scope of the  
12 95 Directive still seems to be somewhat ambiguous. We  
13 saw that it was -- that the Europeans applied it, for  
14 example, to our PNR program, and it took a European  
15 Court of Justice decision finding it not within the  
16 so-called first pillar, and therefore outside of the  
17 scope of the 95 Directive. Then we had to negotiate a  
18 second agreement. There are other DHS programs that  
19 may also be examined under the 95 Directive. So  
20 that's very interesting to us that that is being  
21 looked at.

22 Also, the Data Protection Framework

1 decision. Well, just to continue on the Directive, it  
2 also -- the Directive has this adequacy clause, and  
3 that -- even though there is no -- there's a data  
4 protection framework decision in Europe that applies  
5 to information transfers, transfers of information in  
6 the so-called third pillar, which would be law  
7 enforcement and security. These are European legal  
8 terms, and forgive me if I'm going too fast with this,  
9 or if you need clarification on these points of  
10 European law.

11           So there's this data protection framework  
12 decision that has an adequacy clause, as well. It's  
13 modeled after the 95 Directive. So we're increasingly  
14 seeing the 95 Directive, which had originally been  
15 applied to -- I think in its inception, it was meant  
16 to be applied to commercial transfers of data -- to  
17 work that we're doing.

18           We watch the APEC cross-border privacy  
19 rules. That is, for the most part, something most  
20 relevant to commercial transfers of data. But  
21 clearly, what's happening in the private sector sets a  
22 tone for the negotiations and conversations we have in

1 the public sector.

2 So three activities that we're involved in  
3 that I think might be of particular interest to you  
4 are the work of the High Level Contact Group, I'll  
5 say a few more words about the EU hotel registration  
6 paper that John alluded to in his opening comments,  
7 and then the PNR review that is -- the joint review  
8 that is upcoming. We've actually completed our  
9 internal review of the Automated Targeting System that  
10 houses PNR.

11 I guess I'll start with the High Level  
12 Contact Group and just draw your attention to a  
13 document that I think you should have received ahead  
14 of time, or it would be on the table. It's this EU-  
15 U.S. Summit, June 12, 2008 Report. The High Level  
16 Contact Group is a group that's discussing principles  
17 for information sharing. Yes? Okay. It's in your  
18 packets. So the High Level Contact Group takes place  
19 under what's called the EU-U.S. Justice Law and  
20 Security Ministerial Troika.

21 Now, who makes up the Troika? On the EU  
22 side, it's the Commission, the Council Presidency,

1       which changes every six months; and on the U.S. side,  
2       it's the Departments of Justice, Homeland Security and  
3       State.

4                 In November 2006, there was articulated a  
5       goal of enabling -- of appointing this High Level  
6       Contact Group to explore ways that would enable the EU  
7       and the U.S. to work more closely and efficiently  
8       together in the exchange of law enforcement  
9       information while ensuring that protection of personal  
10      data and privacy are guaranteed.

11                So the group's identification of the  
12      fundamentals or core principles of an effective regime  
13      for privacy and personal data protection was to be the  
14      first step towards that goal, and there had been --  
15      there have been agreements between the U.S. and the  
16      EU. There's the PNR agreement. There are Mutual Legal  
17      Assistance treaties. There is -- the U.S. is a member  
18      of Europol and Eurojust. So building on those  
19      efforts, it was hoped that this High Level Contact  
20      Group could identify these common principles.

21                And we've made, I think, fairly substantial  
22      progress. There are just a few pure privacy

1 principles remaining. One is redress, and the other  
2 is reciprocity and how reciprocity will be applied.

3           It's also unclear at this point what will  
4 be the way forward, whether the goal of this is a  
5 binding international agreement or non-binding  
6 instrument, which would be sort of a political -- you  
7 know, making these principles public and having a  
8 political declaration, and then trying to build these  
9 principles into future agreements between the U.S. and  
10 the EU.

11           The most recent meeting of the JHA occurred  
12 in -- was it in January? I think so -- in January,  
13 and it was decided that there would be one meeting  
14 before the next JHA meeting, which will be in, I  
15 believe, in June. And so right now, we're in the  
16 discussion phases of how -- what the High Level  
17 Contact Group is going to be discussing in this one  
18 meeting that we have under this presidency. With the  
19 EU switching presidencies every six months, we have a  
20 new opportunity to give the ministers reports of our  
21 progress under the High Level Contact Group.

22           I think the biggest obstacle that we have

1 right now in moving forward is not so much the privacy  
2 principles but really the negotiating mandate that the  
3 Commission may get to -- officially, they're not --  
4 the Commission cannot negotiate with us at this time.  
5 These have been discussions. To get a negotiating  
6 mandate requires the permission of the European  
7 Council, and it was anticipated until very recently  
8 that the Lisbon Treaty was going to be in place by  
9 January 1st, and the Lisbon Treaty would have expanded  
10 the EU from -- EU started out as mostly a commercial  
11 area -- to a common area of justice, law and freedom  
12 and security. So that would broaden the authority of  
13 the Commission to do these sorts of negotiations.

14 I'm not an EU expert lawyer. I'm an  
15 American lawyer. Even the Europeans that I talk to  
16 about this are not always clear about what would  
17 constitute -- what needs to fall into place so that  
18 they can have a mandate to negotiate with us and move  
19 forward faster on HLCG towards a solid product.

20 I see there are already lots of questions.  
21 Maybe I should just be quiet and start answering the  
22 questions.

1 I don't know, whoever is first. Lisa, do  
2 you want to start? Or Howard?

3 MR. BEALES: Ramon Barquin.

4 DR. BARQUIN: I have just two questions for  
5 you. First of all, do you have a normal point of  
6 contact counterpart in our embassies, or when you are  
7 involved in these activities, is it just direct from  
8 here? Does someone wear a privacy hat, if you will,  
9 in our embassies?

10 MS. SAADAT: Yeah, that's a really  
11 interesting question. The embassies are always aware  
12 of our travel. We have a couple of what I see as  
13 obstacles in that area. One is that the foreign  
14 service officers change in, change out, and sometimes  
15 we have to -- the institutional memory might not be  
16 too deep, and we have to remind them of what's gone on  
17 in the past.

18 Secondly, some of them are aware of privacy  
19 as an issue, but the State Department does not have an  
20 office that specifically works on privacy. I mean,  
21 the U.S. Government has not approached privacy as a  
22 foreign relations tool. That wasn't behind the

1 Privacy Act or the way our oversight system is set up,  
2 and I think that's reflected in the State Department  
3 not having someone to do that.

4 But I think if Shannon and I could express  
5 one wish for the next year, it would be for improved  
6 coordination among U.S. Government agencies in this  
7 area, because we may not consider it to be a foreign  
8 policy tool, but other countries do, and it's very  
9 hard to be responsive given our current set-up.

10 MS. BALLARD: But also, just for the High  
11 Level Contact Group, we have a DHS attaché in  
12 Brussels, and we have a Justice Department attaché  
13 also in Brussels who follow HLCG activities very  
14 closely. The privacy experts are Washington-based.

15 DR. BARQUIN: The other question is a bit  
16 more. Is there such a thing as an international -- a  
17 Privacy Office international mission strategy, with  
18 goals, objectives? Most of what you're doing is  
19 interacting, engaging, participating, which seems to  
20 be very tactical. But are there a set of goals that  
21 you have laid out internationally that, if you have,  
22 could you share those with us?

1 MS. SAADAT: Well, because we're not --  
2 because the U.S. Government doesn't view privacy as a  
3 foreign policy tool, no. I would say that we're not -  
4 - unlike the Europeans, we're not trying to assert our  
5 model on other countries. It's never one of the lines  
6 in our presentations "And you should do it the way  
7 we do it." We're often in more of the reactionary  
8 mode where we're trying to explain why we do things  
9 the way we do it, and why that's okay given our  
10 political, legal, historical context, and why it's  
11 okay for other countries to do things their way.

12 But, no, we don't have a certain -- we  
13 don't have a particular privacy point that we're  
14 looking to assert.

15 DR. BARQUIN: I'm not looking for a  
16 national (inaudible), but just for more of a specific  
17 function -- like a strategic plan, but just for your  
18 function.

19 MS. SAADAT: Our strategic plan in the  
20 broadest sense would be just to increase understanding  
21 of how the U.S. Government does privacy, and that's --  
22 that may sound like really low-hanging fruit, but it's

1 not. We have to step right back to checks and  
2 balances, three - you know, legislative, judicial,  
3 executive -- in these presentations because there are  
4 very firm ideas about international data protection  
5 commissioners, and a fundamental misunderstanding that  
6 you can't have privacy protections in a system that  
7 doesn't have an independent data protection  
8 commissioner.

9 So I would say, you know, our overriding  
10 goal is really just education.

11 MR. BEALES: David Hoffman.

12 MR. DAVID HOFFMAN: Yeah, I want to thank  
13 you both for taking the time to come and talk with us  
14 today, and to commend the Office. I hear tremendous  
15 feedback when I travel internationally from folks for  
16 their relationships that they've developed with the  
17 Office and how much they get out of it, particularly  
18 with the international visitors who have come to the  
19 Office and actually gotten a tremendous opportunity to  
20 see how the Privacy Office has operationalized privacy  
21 throughout the Department.

22 I also want to commend the Office for its

1 work in examining the very difficult issue of  
2 independence, which you both have touched on, and John  
3 Kropf also touched on, and the double-edged sword that  
4 it is of independence providing an opportunity for  
5 independent thought and speaking -- an organization to  
6 be able to speak its mind, but also creating great  
7 difficulty for an organization to be deeply embedded  
8 within the government constituencies that are actually  
9 trying to accomplish their mission.

10           With that being said, I would recommend  
11 that I actually think that you guys can do more than  
12 just educate. I think there are lessons that the  
13 international community is learning from you when they  
14 come and visit, as I said, and can continue to learn  
15 even more from the way the Department has  
16 operationalized privacy through the individual  
17 components, how deeply embedded that you are getting.  
18 I think it is unique out there in an organization in  
19 which a large part of the mission is law enforcement.

20           And -- I'm actually turning this into a  
21 question, I promise.

22           [Laughter.]

1           MR. DAVID HOFFMAN: That with the impending  
2     implementation of the Lisbon Treaty, and to the extent  
3     now, as I understand it, it will provide an  
4     opportunity for the different political organizations  
5     in Brussels to do more than they've been able to do in  
6     the third pillar with the member states, more than  
7     they could do with the framework decision, which  
8     really only was able to focus on the transfer between  
9     -- of information between the individual member  
10    states, I think -- I'm wondering how you think you  
11    could use the High Level Contact Group discussions and  
12    the other engagements that you've got to really  
13    advance an opportunity to better -- to help the folks  
14    in Brussels better advance privacy within the member  
15    states as they have this new opportunity brought by  
16    the Lisbon Treaty.

17           MS. SAADAT: Well, I think if there is one  
18    principle that we do really emphasize, it's the  
19    transparency principle, and that's something that  
20    comes up; that's really the cornerstone of our system,  
21    is the degree to which our system is transparent.

22           And I've kind of been learning from

1 spending time overseas and having data protection  
2 experts from other countries spend time in our Office  
3 that there are -- in any -- and perhaps this goes for  
4 any government program. There need to be pressure  
5 points. There are pressure points, and the data  
6 protection -- an independent data protection  
7 commission provides one type of pressure point. It  
8 can bring in the attention of the media, for example.  
9 Having an embedded privacy officer is a different sort  
10 of a pressure point.

11 A good system, I would assert, has lots of  
12 pressure points along the way, and maybe that's  
13 another way of saying checks and balances. I think  
14 that through the High Level Contact Group we have  
15 increased understanding about the way, because we have  
16 had to be very responsive to European questions of how  
17 our -- how it all works here.

18 And this kind of actually segues a little  
19 bit into the hotel registration piece. I think the  
20 larger point that we were trying to get at with that  
21 report was that different countries' implementation of  
22 their privacy regimes has different attributes, and

1 one of the attributes of the U.S. system is  
2 transparency, and that that should be how transparency  
3 interrelates with redress. And some of the other  
4 principles can perhaps be -- should be taken into  
5 account when the EU is looking at how it's going to do  
6 privacy in the third pillar.

7 MR. DAVID HOFFMAN: Thank you.

8 MS. SAADAT: You're welcome.

9 MR. BEALES: Dan Caprio.

10 MR. CAPRIO: Thanks, Shannon and Lauren,  
11 for your report. A question really about the ISO work  
12 on privacy standards, and it sort of arises from the  
13 fact that that's non-traditional work for standard-  
14 setting bodies. So, a couple of questions.

15 What other federal agencies are you working  
16 with? I mean, for instance, ITA, NIST, FTC? And sort  
17 of how is that collaboration -- and the process that  
18 feeds into an ISO standard with ANSI really is very  
19 non-traditional for a subject matter like privacy.  
20 And then the second part is what's the timing and the  
21 timetable, and what's the expected outcome?

22 MS. SAADAT: So, on the technical advisory

1 group, NIST is the lead. NIST is always the ANSI  
2 member, and ITA is a participant. We just literally  
3 in the last couple of weeks took this on. The FTC --  
4 and FTC should really speak for themselves, but as I  
5 understand it, standard-setting wouldn't be an  
6 appropriate role for them. And so, although  
7 individuals working at the FTC are very interested in  
8 this work, I'm not sure that a formal role is likely  
9 to come about, and that's really it for the U.S.  
10 Government.

11 I wish there were other U.S. Government  
12 people participating in this because we have a unique  
13 perspective, and it's a lot of -- it's an awful lot of  
14 work. These are thick, complex documents, and Shannon  
15 and I only have so many hours in a day to take this  
16 on.

17 So there are different standards and  
18 different degrees of being - in different standards of  
19 development, different levels of development, and some  
20 of them are at the early stages, and some are much  
21 further along, and some are geared specifically at  
22 biometrics, and others are more general, like the very

1 general privacy standard.

2 I saw last week a privacy reference  
3 document that's a compilation of all privacy document  
4 references in the world, and there was nothing in  
5 there under U.S., which is pretty alarming considering  
6 there are over 700 Federal and state laws. But nobody  
7 had taken it on, and I don't know the answer to why  
8 nobody has taken it on, and Shannon and I will do the  
9 best we can. But we look forward to assistance from  
10 the private sector, or the public sector.

11 MS. BALLARD: Also, Dan, the reason we got  
12 involved in ISO was for exactly that reason. Lauren  
13 and I used to work at Commerce, and so we understand  
14 the role of NIST and ITA within that body. But we saw  
15 that this standard was much less a technical standard  
16 for privacy -- like how do you implement security  
17 safeguards, would seem like an appropriate thing for  
18 ISO to go -- and saw it more as policy-making, you  
19 know, defining what is good privacy and how do you do  
20 privacy, and that's why Lauren and I got so concerned  
21 with it some months ago.

22 And so we have been trying to stay on top

1 of it. We have certainly engaged with Commerce and  
2 the private sector people, but those are a very small  
3 group of people that are on the U.S. delegation to  
4 this particular issue within ISO.

5 MR. CAPRIO: Thank you. I think it's safe  
6 to say it's such a big topic that it's an area that  
7 the committee is very interested in, and obviously  
8 whatever opportunities arise for the committee to be  
9 involved in for industry involvement, those would be  
10 most welcome.

11 MR. BEALES: Lisa Sotto.

12 MS. SOTTO: Thank you. Thank you both for  
13 joining us. I'm going to pick up on Dan's -- I had  
14 the same question, Dan, that you did. And I just want  
15 to urge -- the ISO standard seems to me to be going on  
16 in a kind of -- to call it covert is not quite the  
17 right word, but maybe it is. It's been under cover.  
18 I think many people don't really know that it's been  
19 going on, and we as the United States are one voice of  
20 many, many, many, and there are 27 member states, and  
21 we're one little bitty voice.

22 I have deep concerns about the ISO standard

1 because I think once it's issued as a final standard,  
2 it becomes a global standard, because ISO standards  
3 tend to do that. So I would echo Dan's concern and  
4 offer of this committee to assist in any way we can.  
5 I think it really is incumbent upon those of us, and  
6 few of us as far as I can tell, who are following this  
7 process to clamor a little bit more for some deeper  
8 involvement.

9           One other point that I just want to make --  
10 and I'm sorry I'm not asking questions, I'm just  
11 making points -- is that I've seen an uptick over the  
12 last couple of years in the involvement of this  
13 Office, the Privacy Office, in international matters,  
14 and I just think that's tremendously beneficial. I  
15 would love to see some of the policy work that was  
16 done by the Policy Office at DHS previously shifting  
17 back over to the Privacy Office to the extent that  
18 there are privacy issues involved. I know there's  
19 always been involvement from the Privacy Office, but  
20 not necessarily leadership.

21           So I'm delighted to see what I think is a  
22 bit of a shift in that direction, and certainly the

1 committee offers its help in any way that we can on  
2 the international front. Thank you.

3 MR. BEALES: Could I ask you to go into  
4 your next slide on the global privacy debate? I'd  
5 like to hear a little bit about that.

6 MS. SAADAT: Sure. Well, the global  
7 privacy debate I think is really -- the two tectonic  
8 plates is the European model that sort of imposes,  
9 through the adequacy clause of the 95 Directive,  
10 imposes a European model on other countries, and they  
11 proselytize quite openly; and then there's the APEC  
12 model, which is really geared towards the private  
13 sector but shows that -- it's working towards  
14 demonstrating that there are other mechanisms for  
15 ensuring protection of personal information while  
16 allowing cross-border transfers to occur.

17 And most recently, I've been reading about  
18 the Galway Initiative. And this is an effort I think  
19 that is coming mostly from the private sector, but  
20 it's to talk about accountability as a way forward,  
21 and how could the international community define  
22 accountability in such a way that it could be a

1 mechanism for providing assurance in international  
2 transfers.

3           It has been -- there's to be a conference,  
4 I understand. It's now been taken on by the OECD, and  
5 there's going to be a conference this April. I'm  
6 wondering whether accountability couldn't somehow be  
7 engaged in the public sector as well for information  
8 transfers, to kind of expand it outside of just the  
9 private sector mechanism but possibly in the public  
10 sector as well.

11           So that's something that we're following  
12 and that we'd very much like to participate in, and in  
13 my mind I'm kind of coming up with hmm, how would I  
14 define accountability in our context, and could we  
15 make that work too? So we're closely following that.

16           MR. BEALES: John Sabo.

17           MR. SABO: Thank you. David and Ramon and  
18 Dan, and your responses, and looking at the hotel  
19 report, it's almost as if -- and the DHS Privacy  
20 Office is probably the best collection of effective  
21 privacy professionals in government, I mean in the  
22 U.S. Government, and the points about operationalizing

1 privacy are exactly on target.

2 We have a model that operation-wise is what  
3 are otherwise abstract principles, and there's  
4 certainly that sense in that, well, EU has a lot of  
5 bureaucracy and laws, they don't always have the kind  
6 of robust enforcement that we do, or the application  
7 in an operational environment.

8 So having said that, it seems, though, that  
9 what you're doing in the international office of DHS  
10 is actually putting a toe in the water, but the rest  
11 of the body isn't following. And we've got issues  
12 that we've engendered in the U.S., like we looked at  
13 inspection of laptop data or PNR data itself, or tint  
14 prints versus - Skype -- prints, or prints in general,  
15 which are now being adopted in other countries.

16 So to get back to your wish list comment,  
17 it would seem to me that's exactly what needs to  
18 happen. Someone needs to take informed leadership and  
19 get State and Justice and what other appropriate --  
20 Commerce -- what other agencies of government are  
21 needed, and put together a full-court strategic  
22 initiative. And it seems to me that one of the places

1 that has to emerge from is the Privacy Office because  
2 of your track record and because of your depth of  
3 expertise.

4           So there may be things that the committee  
5 can help with, but it almost seems as if -- you know,  
6 the hotel report is really interesting, and why would  
7 the Privacy Office do this study? It's not as if it's  
8 in conjunction with the collection of data by hotels  
9 for homeland security purposes in Europe, but clearly  
10 you've touched a nerve here.

11           And so I guess my suggestion is to move  
12 forward with it, be more aggressive about working with  
13 other government agencies, especially State and  
14 Justice, and try to move forward a coherent policy in  
15 the absence of a national privacy officer.

16           One other thing you might do is persuade  
17 some of these other bodies that the U.S. model -- and  
18 designate an official to represent the government.  
19 Even though it's not a pure data protection  
20 commissioner, it would have the weight of State, DHS  
21 and other agencies behind it. So just a few thoughts.

22           MS. SAADAT: Just one thing I would -- it's

1 a point well taken. You asked why would this report  
2 come out of -- the hotel registration report come out  
3 of the Privacy Office, and there is a clause in the  
4 PNR agreement that references reciprocity and that the  
5 U.S. should not be held to a standard that the EU  
6 doesn't hold itself to, that there shouldn't be --  
7 that the EU should hold the same -- apply the same  
8 rigor to its own collections as it does to the U.S.,  
9 and I think that was why. So that's in the PNR  
10 agreement specifically, and then more broadly that is  
11 one of the principles under the HLCG that we're  
12 working on.

13 MR. BEALES: I think we have time for one  
14 more question from Lance Hoffman.

15 MR. LANCE HOFFMAN: Thank you, Howard, and  
16 thank you. I also want to join my colleagues in  
17 commending your work and your presentation. It was  
18 very interesting this morning to hear what you had to  
19 say, especially about the ISO efforts.

20 I echo the comments of Lisa and Dan. Real  
21 alarm bells started going off for me when you started  
22 talking about those.

1           I also echo John Sabo's comments in terms  
2 of -- well, actually, U.S. Government, you say in your  
3 slides here, looking forward, U.S. Government  
4 coordination plus private and public partnerships. It  
5 seems like there could be more effort not so much on  
6 DHS' part, but across the rest of the U.S. Government  
7 somehow.

8           So my question really is -- so first I'm  
9 going to again reinforce, please keep an eye on that  
10 because that is somewhat concerning, to me at least.

11           What other U.S. agencies would you like to  
12 see involved besides the ones that are there now? Who  
13 do you think may have a -- and you may want to think  
14 about this -- may have a place at the table but isn't  
15 there yet? What other professional organizations you  
16 might like to see involved, and whether there are  
17 trade groups.? Some of them may already be  
18 represented by Imagine. This is so much under the  
19 radar that some are not and maybe ought to be.

20           MS. SAADAT: Well, I think maybe we should  
21 give it some thought and maybe send you a list or  
22 present the committee with a list of whom we'd like to

1 see involved in the ISO.

2 MS. BALLARD: And just a general comment.  
3 We do work very closely with Justice and State on the  
4 HLCG and other law enforcement counter-terrorism  
5 issues. When we're talking about the global privacy  
6 debate, there's other agencies, the Commerce  
7 Department, FTC, that have quite a lot at stake as  
8 well with privacy issues.

9 But for the public sector, DHS is also a  
10 collector of information. So it certainly impacts us  
11 if there's going to be changes in privacy standards.  
12 We're a government agency. We're also a user of  
13 information. So if one department goes into a  
14 multilateral forum with one objective, the U.S.  
15 Government certainly does need to speak off the same  
16 page and to make sure that we're not saying or doing  
17 something that could adversely impact another  
18 department.

19 So we have begun -- we don't have a formal  
20 name yet, but an international interagency working  
21 group on privacy, trying to look at international  
22 issues, look at what each department or agency is

1 doing internationally in regards to privacy, and we  
2 have begun a dialogue amongst ourselves to try to make  
3 sure that those types of things don't happen.

4 But we'd certainly appreciate your  
5 feedback, your involvement with other departments that  
6 may be doing international work on privacy, to inform  
7 them on these types of issues as well. So, certainly.  
8 Thank you.

9 MR. LANCE HOFFMAN: I'd love to get that  
10 list.

11 MR. BEALES: All right. Well, Ms. Ballard,  
12 Ms. Saadat, thank you very much. It's been a very  
13 interesting presentation and interesting to learn what  
14 you're up to, and a little bit scary to hear about  
15 ISO, but -- and it's perhaps an area that we should  
16 talk to the Privacy Office about where we might be  
17 able to be helpful in that effort.

18 At this point, our schedule calls for a  
19 break. We're running a little bit behind, so I think  
20 we should take our 15-minute break as the schedule  
21 says, and we will resume promptly at 11 o'clock.  
22 Thank you.

1 [Recess.]

2 MR. BEALES: Associate Director for Disclosure and  
3 FOIA program development. He focuses on FOIA policy,  
4 conducts FOIA training, works with the DHS components  
5 to improve FOIA-related processes and procedures, and  
6 he also serves as the FOIA public liaison under the  
7 executive order and the Open Government Act of 2007.

8 Mr. Holzerland, welcome.

9 MR. HOLZERLAND: Thank you.

10 MR. BEALES: We look forward to hearing  
11 about FOIA implementation at DHS.

12

13

14

15

16

17

18

19

20

21

22

1 UPDATE ON FOIA IMPLEMENTATION AT DHS

2 MR. HOLZERLAND: Good morning. First of  
3 all, I'd like to thank everyone for taking the time to  
4 let me discuss FOIA with you today.

5 I would also like to start out by  
6 mentioning that a few years back, when I first took  
7 this position, I spoke with a very large group of  
8 USCIS FOIA employees regarding new initiatives at the  
9 Privacy Office and this kind of thing. I spoke for  
10 about 45 minutes, during which time the audience  
11 looked to be rapt with attention. And at the end,  
12 when I began to take questions, I saw a bunch of hands  
13 raised. And when I called on a person, the first  
14 question was, "And how old are you again? We've been  
15 taking bets back here." So I wanted to stipulate  
16 right up front that, yes, I am as young as I  
17 apparently look.

18 But anyway, we'll dive right into FOIA  
19 here. The need for transparency in government has  
20 been recognized since the early days of our country,  
21 of course. Here we have a piece of a letter James  
22 Madison wrote to Barry regarding the need for an

1       educated citizenry, and I think that ties in quite  
2       well with the current administration's focus on  
3       transparency and the idea that the country as a whole  
4       benefits from having an educated electorate.

5               FOIA, of course, was first enacted in 1966.  
6       It's been amended several times since, most recently,  
7       of course, the Open Government Act of 2007. I'd also  
8       like to note that when the FOIA was signed into law,  
9       quietly over the July 4th weekend in 1966, President  
10      Johnson saw fit to issue a signing statement rather  
11      than hold a traditional signing ceremony. So I think  
12      that was sort of a prelude to what I like to refer to  
13      as 43 years of less than enthusiastic statutory  
14      implementation, which is what we're all here trying to  
15      alter for you.

16             Of course, the FOIA does provide a  
17      statutory right of access to Federal agency records.  
18      It presumes that records are available to the public,  
19      unless they are specifically exempted by one of the  
20      nine exemptions or excluded from the statute entirely.

21             The purpose, as we mentioned, was to ensure  
22      an informed citizenry and prevent secret law, hold the

1       governors accountable to the governed, of course.

2                 Now, we do follow DOJ guidance in the  
3       Executive Branch. They're the key agency for FOIA  
4       implementation. But within the Privacy Office, we do  
5       set and implement FOIA policy DHS-wide.

6                 Talk a little bit about the structure of  
7       our Office. I'm sure most of the folks in this room  
8       are familiar with the DHS Privacy Office, which was  
9       created by Section 222 of the Homeland Security Act.  
10       But within the Privacy Office, we are bifurcated into  
11       two separate and distinct functional areas, privacy  
12       and disclosure. Within the disclosure group, we are  
13       further divided into separate practice areas. We  
14       have, of course, a -- the Chief Privacy Officer serves  
15       concurrently as the Chief FOIA officer for DHS. We  
16       also have a Deputy Chief FOIA officer.

17                 Just below the chief, the deputy chief FOIA  
18       officer -- excuse me -- on the org chart, we are  
19       divided into operations and policy and program  
20       development areas.

21                 You'll also notice that we have a dotted  
22       line reporting relationship with the FOIA offices DHS-

1 wide. The FOIA officers report to their component  
2 heads, but they also have a dual reporting requirement  
3 to the Chief FOIA Officer for policy purposes and for  
4 reporting purposes. And that, of course, includes our  
5 annual report to the Attorney General. We also  
6 collect information from the FOIA offices on a weekly  
7 and monthly basis, as well.

8 Our Office does process FOIA requests --  
9 excuse me -- requests for records of the Secretary,  
10 the Deputy Secretary, and the Executive Secretariat,  
11 just to give you an idea of how we're structured. But  
12 I also want to mention that the Office has grown by  
13 leaps and bounds since the day I walked into it.

14 Under the stewardship of the last Chief  
15 Privacy and FOIA Officer, we started out with one FTE  
16 when I -- excuse me -- full-time employee, or full-  
17 time equivalent -- excuse me -- when I walked in the  
18 door. But we were able to take on two positions that  
19 Vania Lockett, the Associate Director of Operations,  
20 and myself currently occupy.

21 Since that day, we have been able to gather  
22 an eclectic group of individuals with very different

1 backgrounds and experiences. We have currently nine  
2 FTE within the FOIA side of the Office, and within  
3 that group we have folks who came from various  
4 agencies at the Department of Defense, someone with  
5 U.S. Agency for International Development and FDA FOIA  
6 experience. We have somebody who we stole -- we were  
7 lucky enough to steal from the Secret Service. So we  
8 have assembled -- we've hand-picked quite a team to  
9 help us not only process requests at the headquarters  
10 level, but help us oversee the operations and  
11 activities of the Departmental components as well.

12 I'll move on here. Now, the slides that  
13 I've assembled today basically consist of a brief  
14 overview of recent developments in FOIA legislation,  
15 as well as executive orders and memoranda.

16 First, I won't spend a lot of time on E-  
17 FOIA since we are so far out in terms of time here,  
18 but the E-FOIA amendments were enacted in 1996. It  
19 required us, of course, to create a reading room  
20 category of records, submit annual reports to the  
21 Attorney General regarding the activities of FOIA  
22 operations and, most importantly, make all records

1 electronically available, those that were created  
2 after November 1st, 1997.

3           Also, the E-FOIA requirements did require  
4 that agencies promulgate regulations to allow  
5 requests, certain requests to be expedited. And  
6 essentially, it also required us to provide notice of  
7 whether or not we were going to grant expedited  
8 processing within 10 days. Of course, DHS is in  
9 compliance with -- in full compliance with the E-FOIA  
10 amendments 13 years out.

11           I would like to mention, of course, the  
12 executive order that was issued by former President  
13 Bush in December 2005. This was the first game-  
14 changing development, I believe, since the E-FOIA  
15 amendments of '96. Essentially, the executive order  
16 required that agencies look at FOIA operations as a  
17 customer service sort of piece of our business. It  
18 required that FOIA programs be citizen-centered and  
19 results-oriented, which were not two attitudes that I  
20 believe were very apparent when dealing with  
21 submitting FOIA requests to Federal agencies.

22           And I should mention as a -- since we are

1 talking disclosure here, my background is as a  
2 journalist. So I've been on the short end of the  
3 stick in terms of trying to access information. So I  
4 did want to mention that, as well.

5 The executive order also required that  
6 agencies designate a Chief FOIA Officer, I believe at  
7 the assistant secretary level or higher. Of course, I  
8 mentioned that at DHS the Chief Privacy Officer wears  
9 the dual hat as the Chief FOIA Officer, as well.

10 One of the most important pieces as far as  
11 customer service goes was the requirement that  
12 agencies establish one or more FOIA requester service  
13 centers and designate one or more FOIA public  
14 liaisons. We at DHS have -- some components have more  
15 than one FOIA requester service center, but all have  
16 at least one, and I am the public liaison for the  
17 Department. So I serve as the supervisory official to  
18 whom FOIA requesters can appeal should they encounter  
19 customer service challenges at our various components.

20 Agencies were also required to submit FOIA  
21 improvement plans to the Department of Justice. We  
22 here at DHS compiled a FOIA improvement plan which our

1 former deputy secretary basically referred to as  
2 insufficiently aggressive, and we took that statement,  
3 looked at it as a challenge, and compiled a revised  
4 FOIA improvement plan which had, we think, better and  
5 more measureable targets for DHS to reach. It was  
6 more specific.

7           The FOIA officers at our various components  
8 also -- not only do they report to us on a weekly,  
9 monthly, and annual basis, but they were required to  
10 report to us on success meeting milestones related to  
11 the FOIA improvement plan, or lack thereof. But that  
12 is something that we at the Privacy Office have been  
13 keeping a close eye on since those plans were  
14 submitted.

15           The Open Government Act of 2007 essentially  
16 changed the game in a few more ways. First of all,  
17 the routing requirement I think is very important  
18 from a customer service perspective. Basically, that  
19 means that the 20 business day clock we have to comply  
20 with a FOIA request begins either the day the  
21 appropriate DHS component receives a FOIA request or  
22 no greater than 10 days after any component receives

1 the FOIA request.

2           Previously, agencies were -- though this is  
3 not a best practice, clearly, agencies were entitled  
4 to simply let a request -- advise a requester that  
5 they should submit their request to the appropriate  
6 component. But this sort of -- first of all, it's  
7 obviously customer friendly, but it also puts a little  
8 bit more pressure on components to add some urgency to  
9 the routing of requests. No longer can this be done  
10 at a leisurely pace.

11           Also, I think this is an interesting  
12 development, too. When requesters contact the service  
13 center, we are required to provide an estimated  
14 timeline for processing the request. It is, of  
15 course, an estimate, but we do try and meet those  
16 estimates.

17           So theoretically, requests cannot be  
18 sitting in the queue indefinitely. We have to have a  
19 measureable target for getting it out the door, and we  
20 do have to advise the requester of how we plan to  
21 process it in terms of whether records are voluminous  
22 or there's other circumstances that require us to take

1 longer than 20 business days. At least we've been  
2 encouraged to communicate more openly with the  
3 requester about the process.

4           So I think this adds a little bit -- this  
5 piece in particular adds a little bit more  
6 transparency to the transparency, if you will. We do  
7 try and let the requesters know exactly what's going  
8 on with their given request at whatever point in time  
9 they contact us.

10           Also, the Open Government Act of 2007  
11 requires more granularity in terms of our reporting to  
12 the Attorney General and Congress. We've always  
13 reported on the number of pending requests, the number  
14 of requests processed, the number of times a given  
15 exemption is claimed, et cetera. But now we're  
16 required to not only report on pending requests but  
17 backlogged requests, pending being any request that is  
18 currently open or for which the agency has not taken  
19 final action in all respects. But backlogged requests  
20 means any open requests that are open longer than 20  
21 business days. So those are two separate and distinct  
22 pieces of information, and I think it's very important

1 when you're looking at the annual report to take that  
2 into account.

3 Also, the Act established a definition of  
4 representative of the news media, and it was a very  
5 broad definition. It does specifically include --  
6 it's intended to specifically include bloggers and  
7 other new media types, as Congress left this open. As  
8 new media types develop, we are clearly instructed to  
9 include such members of the media as media.

10 Of course, this is important for purposes  
11 of fee assessment. In terms of requests for expedited  
12 processing, that may come into play. Obviously,  
13 Congress intended to favor those who disseminate  
14 information to wide audiences, and we need to be  
15 expansive and inclusive rather than exclusive when  
16 we're trying to define who is and who is not media.

17 Also, and I think this was a very exciting  
18 development from an open government perspective,  
19 requiring that agencies pay out attorney fees from  
20 FOIA suits from our own appropriations rather than the  
21 general judgment fund over at Treasury. I think that  
22 is a tool which will encourage program offices to

1       comply if they are worried that non-compliance with a  
2       FOIA request may cost their program money. So I think  
3       that is a very interesting development, as well.

4               I saw a -- recently I saw an opinion where  
5       CIA lost a case and was forced to pay \$350,000 in  
6       attorney's fees, and that is something that I have  
7       screamed long and loudly from the rooftops to our  
8       component FOIA offices and program offices when I'm  
9       conducting training, that clearly you don't want to be  
10      the person who costs the Department significant funds  
11      due to non-compliance with a FOIA suit. So I think  
12      that's a tool that, fortunately or unfortunately, we  
13      can use to encourage our program offices to help us  
14      comply with the FOIA.

15              Also, one of the pieces of this legislation  
16      that also went into effect on 12/31/08 is that we are  
17      prohibited from assessing certain fees if we fail to  
18      comply with FOIA deadlines. Again, that's -- from a  
19      FOIA Office perspective, that is another tool by which  
20      we can convince our program offices to turn over  
21      responsive records or make recommendations on  
22      releasability in a timely manner, which has been a

1 challenge in years past.

2           Also, I know that the Act did establish an  
3 Office of Government Information Services, which  
4 Congress intended to place within NARA. I know there  
5 was wrangling at this time last year between the White  
6 House and Congress over where that office would  
7 actually reside. Our former president's budget had  
8 placed that office within the Department of Justice.  
9 This met with resistance on the Hill, clearly.

10           But I was pleased to notice that about a  
11 month ago, the director's position for the Office of  
12 Government Information Services was advertised. So it  
13 appears that this office will get up and running, and  
14 I think this office is going to play a role similar to  
15 that of the FOIA public liaisons, and I say that  
16 because this office is intended to act as a sort of a  
17 FOIA ombudsman and informally resolve disputes between  
18 agencies and requesters.

19           To relate that to my own role as the public  
20 liaison, essentially I like to know -- when requesters  
21 contact our office, I like to have any customer  
22 service or FOIA in general-related issues brought to

1 our attention as early as possible. The minute a  
2 requester encounters trouble with a program FOIA  
3 office at a DHS component, I love to know about it.  
4 The sooner we know, we may be able to step in and help  
5 resolve whatever the dispute is amicably, which  
6 benefits the agency, of course, not to spend time and  
7 money on litigation, and it benefits the requester  
8 community as well, being able to have us facilitate  
9 access to records in a timely manner or work with them  
10 to resolve scope issues, or whatever the issue may be.  
11 We're happy to do that. And I think that the Office  
12 of Government Information Services is going to provide  
13 support to those of us who serve as the FOIA public  
14 liaisons and take on that role at executive agencies.

15 Also, the Open Government Act clarified  
16 that the definition of a record does, of course,  
17 include any information maintained by a contractor for  
18 the government for purposes of records management. We  
19 have been operating under that assumption for a long  
20 time, but it was also clarified in the Open Government  
21 Act.

22 The most recent development in terms of

1 overall FOIA operations Executive Branch-wide was the  
2 memorandum issued by President Obama on day one in  
3 office, and over the course of the last year or so,  
4 I've been advising our different program offices and  
5 those who I have trained on the FOIA that whatever  
6 administration it was that was going to be coming into  
7 D.C. in January, I believed was going to be a little  
8 bit more transparent than the last. And I was very  
9 excited that the President took the time to issue such  
10 a memo from his own desk, and especially on day one in  
11 office. I was expecting this administration to be  
12 very transparent, but you could have knocked me over  
13 with a feather when I saw that this was issued on day  
14 one, and I think that it is a game changer.

15 Typically, the last few administrations  
16 have had their respective Attorneys General issue FOIA  
17 policy guidance, I believe around the October  
18 timeframe in the last two administrations. It usually  
19 takes some time to get around to issuing such  
20 guidance. But for this memo to come from the desk of  
21 the President himself, it really is a very exciting  
22 development from the open government perspective.

1           Of course, this memo reaffirmed our  
2           commitment to accountability and transparency. The  
3           language in this memo was very clear. The President  
4           quoted Justice Brandeis, I believe, when he said that  
5           sunlight is said to be the best of disinfectants, and  
6           that we are to administer the FOIA with the clear  
7           presumption that, in the face of doubt, openness  
8           prevails.

9           Now, in his -- I believe when the President  
10          was making remarks that same day, while swearing in  
11          some of his senior staff, he did take time to mention  
12          the FOIA during these remarks, and he very  
13          unequivocally stated that the White House stands on  
14          the side of those seeking information rather than  
15          those who are seeking to withhold it. And I think  
16          that is a very clear policy shift from what we've been  
17          working under the last couple of years here.

18          Of course, also, the President very  
19          specifically stated that agencies should take  
20          affirmative steps to make information public, and that  
21          we need to leverage modern technology to do so. One  
22          of the areas that I focus on within the Privacy Office

1 is the electronic reading room and the FOIA public  
2 website. And we do want to use such tools to post as  
3 much information proactively as possible.

4 And we have several DHS components which  
5 really tend to follow this kind of philosophy. I can  
6 point to, for example, the Office of Inspector General  
7 proactively posts audit reports, inspection reports,  
8 and this kind of information on their website. And  
9 they don't -- most importantly, citing back to the  
10 President's memo, they don't wait for FOIA requests to  
11 disseminate this information. I think that's a very  
12 important example for other DHS components to look at  
13 and to follow.

14 Also, the President's memo directs the  
15 Attorney General to issue new FOIA guidance, which we  
16 in the FOIA community are anxiously awaiting. We're  
17 looking forward to that, we're told, in the very near  
18 future. We've not been given a specific date, but  
19 we're looking forward to that this spring, and that  
20 will help us provide specific guidance to our program  
21 offices on how to implement the new policy.

22 Obviously, the clear presumption that, in

1 the face of doubt, openness prevails, the President  
2 was clear that that policy supersedes the former  
3 policy that we were living under, the Ashcroft policy  
4 of clearly - or excuse me -- carefully applying FOIA  
5 exemptions, and if we have a sound legal basis for  
6 doing so, to withhold information. So the President  
7 was pretty clear that the new policy immediately  
8 supersedes the former Attorney General's policy and  
9 that we are to begin operating under this assumption,  
10 or presumption, right away. So we're very excited  
11 about this new development.

12 Now, I have a couple of slides here that  
13 I'd like to share both with those in our program  
14 offices, and I say that -- I specifically mean those  
15 that are not FOIA offices within the Department. I  
16 have a couple of slides that show, sort of from cradle  
17 to grave, the life cycle of a FOIA request.

18 And to be very clear, I don't put these  
19 slides in here in order to gain sympathy or anything  
20 of that nature, but I want to make it clear what kind  
21 of steps we do have to go through to process a FOIA  
22 request, because as FOIA public liaison I try to spend

1 as much time as possible educating requesters on how  
2 the process works. I think it's important the  
3 requester community knows what we go through, because  
4 an educated requester -- it works well, to everybody's  
5 advantage, if the requester knows the FOIA, knows how  
6 the process works; and we can scratch each other's  
7 back, I think, when we have that kind of situation.

8           So, of course, when we receive a FOIA  
9 request, we have to examine it on its face and go  
10 through some procedural steps before we even task it  
11 out for a search. We may have to determine the fee  
12 category of the requester, whether the requester is  
13 commercial, media, or falls into the "All Other"  
14 category. Of course, that is an issue which we can  
15 and have had to litigate. So it's not always clear  
16 and cut and dried right on the face of the request.

17           We do also have to resolve any outstanding  
18 scope issues regarding the request. Oftentimes,  
19 requesters will not target their request because they  
20 are worried that if they don't phrase their request  
21 broadly, that we may exclude or not find certain  
22 records that they wish to have access to. So we do

1 spend a lot of time communicating with requesters via  
2 phone, email, letter, or any other method in order to  
3 figure out what it is they're seeking. And  
4 oftentimes, we're able to narrow the scope of requests  
5 or target them a little bit better so we can conduct a  
6 better search.

7           For example, one of my favorite requests  
8 that I've ever received was a gentleman sent me a  
9 letter saying, "I request access to and copies of a  
10 list of everything we're not allowed to know."

11           [Laughter.]

12           MR. HOLZERLAND: And so that one, I was  
13 able to speak with the gentleman on the phone and I  
14 sent him the URL for our website and said, "Here is  
15 the list of the nine FOIA exemptions. There's the  
16 list of everything you're not allowed to know." And  
17 that was what he was seeking, but it wasn't very clear  
18 on the face of the request what he meant. But through  
19 a five-minute chat we were able to resolve the whole  
20 thing. Request withdrawn.

21           At any rate, we do also assign tracking  
22 numbers to every request received. The Open

1 Government Act requires that we assign a tracking  
2 number to all requests that are going to take longer  
3 than 10 days to process. But for purposes of making  
4 sure that nothing falls through the cracks and that  
5 we're reporting accurately at the end of the fiscal  
6 year, we do assign a tracking number to every request  
7 received.

8 We then fire off a letter at this stage to  
9 the requester advising them that we did receive your  
10 request, here's the tracking number, here's our  
11 contact information in case we need to get hold of  
12 each other about this request, and we let them know at  
13 that point how we interpreted their request. Here's  
14 what we think you're asking for. If there are any  
15 issues with respect to our interpretation, it's the  
16 requester's opportunity to clarify or correct our --  
17 if we misjudged the request on its face.

18 At this point, we also have to task out the  
19 request to the appropriate program office that may  
20 have responsive records, assuming they exist. It's  
21 not always clear, of course. The requester doesn't  
22 always know who has the records. We don't always know

1 who has the records. But we sure do our best to find  
2 out. And this is another reason why having an  
3 educated requester, having them submit a targeted  
4 request and know what they're looking for is very key.  
5 It helps us make sure we task the appropriate parties  
6 and that we cover the waterfront in terms of making  
7 sure we locate all responsive records.

8           At that point, the program office, the  
9 appropriate program office that owns the records would  
10 then provide the records to the FOIA office and advise  
11 us of any recommendations they may have with respect  
12 to the releasability, or lack thereof, regarding the  
13 records. And at that point we may have to hash out  
14 some issues with the program offices. We don't always  
15 agree.

16           There's a tendency, we've noticed, of folks  
17 to be over-zealous in trying to apply the exemptions  
18 when they turn over responsive records. They may tell  
19 us it's all exempt under X exemption. Well, that's  
20 not specific enough. We need to articulate -- we need  
21 them to articulate for us the reasons why a given  
22 piece of information might be exempt. We can't just

1 blanket apply exemptions to whole records on a general  
2 basis.

3           So we do have to engage the program  
4 offices, communicate with them, which can be a multi-  
5 step sort of process. Once we locate responsive  
6 records, we may find records that do not belong to the  
7 Department. We may find other Federal agency records,  
8 and we may be required to consult with another agency  
9 to get their release -- their determination on the  
10 releasability of a given piece of information, or we  
11 may have to refer the request in its entirety. So  
12 there are a lot of administrative considerations that  
13 we have to -- that we go through before the final  
14 steps here.

15           After all is said and done, after all of  
16 the procedural minutiae is worked out, we do send a  
17 letter to the requester itemizing all responsive  
18 records, assuming that we did locate responsive  
19 records, and letting them know, letting the requester  
20 know how many -- how much information we are releasing  
21 in full, releasing in part, or withholding in full.  
22 And, of course, we do have the potential for an appeal

1 or litigation. Of course, the appeal or litigation  
2 can also appear sort of out of order earlier in the  
3 process.

4 One of the questions I've been asked in  
5 past appearances such as this one is what our strategy  
6 is regarding litigation, and simply put, my strategy  
7 is to avoid litigation to the extent possible.  
8 Obviously, litigation for -- litigating over  
9 constructive denial, complaints received for that, for  
10 not responding to a FOIA request, I mean, those are  
11 the kind of battles we don't need to fight. Those are  
12 easily avoidable, and we try and do that to the extent  
13 possible.

14 Of course, a requester can appeal any  
15 adverse determination we make; that is, either that we  
16 did not locate records, that we denied a fee waiver,  
17 expedited processing, or that we withheld records in  
18 full or in part.

19 So it's -- there are a lot of steps. There  
20 are a lot of permutations of the ways these steps can  
21 occur, and it can get very interesting. These steps  
22 -- I like to refer to FOIAs -- I tell people that

1 they're all like snowflakes. There are no two alike --  
2 there are very few situations where we can say we  
3 always do X. FOIA requests tend to be very unique and  
4 may require these steps to happen sort of out of  
5 order.

6           And as I mentioned earlier, we do report --  
7 we do compile a report for the Attorney General at the  
8 end of the fiscal year which details, of course, the  
9 number of times we -- excuse me -- the number of  
10 requests received, processed, the number of pending  
11 requests, backlogged requests, average and median  
12 response times, our costs -- so that would be overhead  
13 as well as fees collected. Information regarding the  
14 agency's 10 oldest open FOIAs is included in the  
15 annual report, as well as other pieces of information.

16           I don't mean to over-simplify the annual  
17 report. It's a significant amount of information in  
18 one document, but that's it in a nutshell.

19           I don't plan to spend too much time on the  
20 exemptions here. I just added this for those who may  
21 be unfamiliar. But I would like to point out that the  
22 most frequently invoked of these exemptions in fiscal

1 year 2008 were exemptions B2, B6, and B7c, I believe.  
2 So, of course, 6 and 7C being the privacy-related  
3 exemptions. You'll notice the absence of 8 and 9 in  
4 the annual report. Those are typically not used at  
5 the Department. In fact, I think 8 was used once, and  
6 it was a typo. So it appeared once since we opened  
7 our doors on the annual report.

8 Notice, though, that there is no Exemption  
9 10 for Dumb and Embarrassing. That is one thing that  
10 I always like to point out to our program offices, to  
11 our FOIA offices, and the President very specifically  
12 mentioned this in the FOIA memo that he issued on  
13 January 21st of this year, meaning the FOIA does not  
14 allow us to withhold information simply because  
15 disclosure of a given record might be embarrassing to  
16 government officials, might reveal failures, or might  
17 be embarrassing to the agency. So I think that is a  
18 very important thing to note, and that's another  
19 tidbit that I shout long and loudly from the rooftops  
20 to our program offices when I take my show on the road  
21 and conduct FOIA training.

22 And that actually wraps up the slide

1 portion of the presentation. At this point, I would  
2 be most happy to take any questions that the committee  
3 or the public may have.

4 MR. BEALES: All right. Thank you very  
5 much, Mr. Holzerland, for your presentation.

6 I guess we will start with Richard Purcell.

7 MR. PURCELL: Thank you. Thank you for  
8 your presentation, Mr. Holzerland. Let's talk about  
9 Exemption 6 for a little while. That's the one, of  
10 course, that will be first on my list of trying to  
11 understand and get my head around how general privacy  
12 criteria might be applied to a request for  
13 information, and what that criteria might be, and how  
14 it might be defined. Can you help with that, please?

15 MR. HOLZERLAND: Certainly. Certainly.  
16 With respect to Exemption 6, the criteria that we have  
17 to employ here, we have to do a balancing test. We  
18 have to essentially decide if the disclosure of the  
19 information would cause a clearly unwarranted invasion  
20 of personal privacy. That's a pretty high standard.

21 As a side note, the standard in Exemption  
22 7C, which is the law enforcement privacy exemption, is

1 a little bit easier to meet. The standard in  
2 Exemption 7C is that the disclosure of the record  
3 could reasonably be expected to cause an unwarranted  
4 invasion of personal privacy. So it's a little bit  
5 lower standard. It's easier to apply 7C.

6 6 is a little bit tougher, and when we're  
7 applying Exemption 6, we have to decide does the  
8 public interest in a given piece of information  
9 outweigh the individual's private interest in the  
10 withholding of the record. And when the scale is  
11 tipped towards privacy, we do err on that side. We  
12 have to be very -- we have to be careful with the  
13 disclosure of information that identifies individuals.

14 It's important to note for requesters that  
15 when we conduct this balancing test, we have to  
16 determine whether, as I said, the public interest  
17 outweighs the privacy interest of the individual in  
18 question. That doesn't mean that the requester's  
19 private interest in the information is factored in.  
20 We have to consider whether the public at large would  
21 benefit from the disclosure of the information.

22 MR. PURCELL: If I may follow up, fine.

1 But the criteria for how you define personal privacy  
2 is of vital importance to us because, clearly, some  
3 very great number of FOIA requests that are granted  
4 contain personally identifiable information. Somebody  
5 wrote a memo. Somebody is mentioned in a record. I  
6 mean, there's got to be a lot of PII in granted  
7 requests, but they don't rise to the level of being an  
8 invasion of privacy. So the definition and criteria  
9 around that would be helpful for us to understand.

10 MR. HOLZERLAND: Well, and that's another -  
11 - that's an area - as I mentioned FOIA is very  
12 subjective. It's not always crystal clear how we can  
13 define these sort of issues. One of the areas that we  
14 often struggle with is what does -- what encompasses  
15 -- what does PII encompass, and that's why we do err  
16 on the side of privacy if we have doubt.

17 But defining what is personal identifiable  
18 information is -- it's often debated. Sometimes, for  
19 example, clear examples would be Social Security  
20 numbers, home addresses, that kind of -- those kind of  
21 obvious examples of PII. Sometimes we withhold -- we  
22 may have to withhold things that wouldn't obviously

1 fall under the definition of PII but that may identify  
2 or be linkable to a particular individual. Sometimes  
3 -- well, I'm trying to think of a good example.

4           There have been instances where I've  
5 withheld information about, in a law enforcement  
6 record, about what state a particular individual holds  
7 a driver's license in, either referring to several  
8 individuals -- even though we're withholding the  
9 identities of those several individuals, only one  
10 person may come from a given state. So in order to  
11 assure that the rest of our applied exemptions make  
12 sense and work, we may withhold -- we may err on the  
13 side of withholding a little bit of additional  
14 information so that there's no chance that you could  
15 reverse engineer the identity of the individuals whose  
16 names were withheld.

17           MR. PURCELL: So do you do that by a  
18 redaction process as opposed to withholding the record  
19 itself?

20           MR. HOLZERLAND: Correct. No, we do try  
21 and segregate. I want to be very clear about that.  
22 We try and release all segregable information. We do

1 -- the philosophy I try and live under here is maximum  
2 disclosure, minimum delay. The delay part is not  
3 always avoidable. But we do try and segregate out as  
4 much information as we can possibly release. Does  
5 that better --

6 MR. PURCELL: I'm still kind of looking for  
7 some criteria, but I'm not sure that that's  
8 necessarily available.

9 MR. HOLZERLAND: There is not a clear-cut  
10 set of criteria. The answer is it depends. We do try  
11 and apply the same sort of standards that our  
12 colleagues on the privacy side of the Office would,  
13 and we do consult with our other half, the other side  
14 of our coin here, in the privacy side of the world, in  
15 order to figure out if a given piece of information  
16 may be PII. We do have to wrestle with it sometimes.

17 MR. BEALES: David Hoffman.

18 MR. DAVID HOFFMAN: I just would like --  
19 thank you for coming in and explaining this to us.

20 MR. HOLZERLAND: Sure.

21 MR. DAVID HOFFMAN: It's actually been very  
22 helpful to understand the process. I would actually

1 like to probe on this just a little bit more. Is  
2 there any guidance document that has been issued, to  
3 your knowledge, by any part of the U.S. Government  
4 defining how to do that balance and how to measure  
5 what the impact to the individual should be?

6 MR. HOLZERLAND: Well, the courts have  
7 weighed in on this question at various points in time.  
8 But I can mention that OPM, for example, has weighed  
9 in on what constitutes personally identifiable  
10 information with respect to Federal employees, what is  
11 and is not -- what kind of information should and  
12 should not be typically released about Federal  
13 employees. That's one example. Things like our  
14 names, duty stations, salaries, that kind of  
15 information is typically, in most cases, releasable.

16 MR. DAVID HOFFMAN: Can I just follow up  
17 and probe on that? It sounds as if there is, to your  
18 knowledge, no document that provides guidance to  
19 individual FOIA officers in the government about how  
20 to actually do this balance of measuring the impact on  
21 the individual's privacy versus the benefit to be  
22 gained. And I'm just wondering, since the Attorney

1 General has been called upon to issue guidance by the  
2 President, of whether that would be something that the  
3 Department ought to be asking the Attorney General to  
4 take a look at and provide better guidance on.

5 MR. HOLZERLAND: Well, and this is a -- I'm  
6 glad you mentioned the Attorney General. Under the  
7 Department of Justice, there's the Office of  
8 Information and Privacy, which does provide FOIA  
9 guidance to the Executive Branch. The DOJ Office of  
10 Information and Privacy does put out a FOIA guide. I  
11 believe every two years they put this out, and it's  
12 extensive. It provides pretty clear guidance on how  
13 to apply all of the exemptions. It provides updates  
14 on recent court opinions or updates, developments that  
15 may happen in between the guide's issuance.

16 So that does -- that may be sort of the  
17 seminal piece of guidance that we look to on a daily  
18 basis in terms of applying all of the exemption  
19 criteria.

20 MR. PURCELL: And you believe that within  
21 that guidance there is specific guidance on how to  
22 handle this particular issue? That might be helpful

1 for someone in the Privacy Office to be able to  
2 provide the committee with that so that we could take  
3 a look at that.

4 MR. HOLZERLAND: There is a chapter, for  
5 example, devoted entirely to Exemption 6 and its  
6 application. That might be -- that might fit the bill  
7 of what you're looking for, and we'd be happy to  
8 provide that.

9 MR. DAVID HOFFMAN: That would be great.  
10 Thank you.

11 MR. HOLZERLAND: Certainly.

12 MR. BEALES: Ramon.

13 DR. BARQUIN: I just wanted to understand  
14 better the -- behind the whole thrust here of FOIA and  
15 what serves the public, and that's a distinction  
16 between what a FOIA requester is asking about  
17 themselves and/or anything else. I mean, is there in  
18 the FOIA intent a positive posture toward letting an  
19 individual know what the government holds about that  
20 individual, to correct it, to whatever? I mean, I'm  
21 just trying to get that aspect of it.

22 MR. HOLZERLAND: Absolutely. When -- and

1 we do -- probably the bulk of the -- I don't have  
2 specific numbers, but the bulk of requests received by  
3 DHS this past year, for example, would be first-party  
4 requests from individuals asking for records on  
5 themselves, and we do -- when those -- when responsive  
6 records are clearly within a system of records, we not  
7 only process a first-party request under the Privacy  
8 Act, but we also put our FOIA hat on and look at it  
9 under the -- do a FOIA analysis on a given record, and  
10 it's best policy and best practices to provide the  
11 requester the greatest amount of information on  
12 themselves as we possibly can.

13           So, in other words, the requester always  
14 gets the benefit of the statute, whichever statute has  
15 the more liberal release requirement in their  
16 circumstances.

17           DR. BARQUIN: Just to follow up on that,  
18 then, because this converges very directly with the  
19 whole issue of redress. In other words, I find out  
20 through FOIA that I may be somewhere, and then how do  
21 you then interact with the redress functions within  
22 the Department and in the components?

1           MR. HOLZERLAND: Well, actually, I in  
2 particular as the FOIA public liaison end up directly  
3 or indirectly involved in these kind of issues on a  
4 routine basis. Oftentimes a requester will seek  
5 information on themselves and they'll get the  
6 information, they'll receive the response to their  
7 request, and if they have questions about it or  
8 they're concerned about information that's contained  
9 in the records, they'll contact our office.

10           And while we don't -- while I specifically  
11 on the FOIA side don't -- we don't exactly directly  
12 get involved in the redress process, we do connect  
13 them with the privacy officer or the privacy point of  
14 contact at the component in question and make sure  
15 that they have an opportunity to submit a request for  
16 amendment or whatever of the given record.

17           MR. BEALES: Joanne McNabb.

18           MS. McNABB: Thank you very much for your  
19 report. Does one of these exemptions cover  
20 information security information? That is,  
21 information on the Department's information security  
22 systems?

23           MR. HOLZERLAND: There could be -- I can

1 say that several exemptions would be applicable. It  
2 would depend on the record. But, for example, we  
3 often apply Exemption (b)(2)(high) to information that,  
4 let's say, well, the release of it would allow  
5 somebody to circumvent a law or a regulation.  
6 Obviously, if they had the manual of, say, how to hack  
7 into DHS network and extract PII or other information,  
8 that would clearly be a negative situation.

9 That might be an exemption we would apply.  
10 It would depend on the record, basically. But, yes,  
11 we can apply one or more exemptions to these kind of  
12 situations.

13 MS. McNABB: Which other ones would you  
14 normally think might apply?

15 MR. HOLZERLAND: When you say information  
16 security, what specific kind of records are you  
17 talking about?

18 MS. McNABB: Well, let's say request for  
19 information on vulnerabilities in systems.

20 MR. HOLZERLAND: Well, vulnerabilities,  
21 definitely high 2. There may be -- depending on if

1 the records, say, are clearly law enforcement records,  
2 we may be able to apply 7E, techniques, techniques by  
3 which we might protect these kinds of information.  
4 That might be one that would apply. If the records  
5 are classified, then, of course, there's B1, and we  
6 have no discretion there. We have to withhold such  
7 records. But again, it does depend.

8           And we do try -- if we're going to have to  
9 withhold a piece of information and we can apply more  
10 than one exemption, we usually do. Obviously, only to  
11 the extent we have to, but if we can apply more than  
12 one exemption, it does make more sense. It's more  
13 easily defensible on appeal or in litigation if we've  
14 applied more than one. That way, if one exemption is  
15 overturned on appeal or in litigation, then we may  
16 still be able to protect that information under what's  
17 left.

18           MS. McNABB: Thank you.

19           MR. HOLZERLAND: Certainly.

20           MR. BEALES: Renard Francois.

21           MR. FRANCOIS: Thank you very much for your  
22 time and presentation. And one of the things that I

1 wanted to ask you about picks up on Richard's point  
2 about Exemption B6. And you had mentioned that you  
3 evaluate whether the public interest in disclosure  
4 outweighs the individual interest in privacy, and I  
5 was wondering if you could articulate for us just some  
6 of the factors that you use in balancing those  
7 competing interests.

8 MR. HOLZERLAND: One piece of this puzzle  
9 would be clearly media attention. We may factor that  
10 in. Is this a hot topic that has a lot of public  
11 interest at the moment? Has this appeared on the  
12 news, blogs, this kind of thing? Is this something  
13 that the public has been greatly concerned about?  
14 It's not always crystal clear. Of course, you know,  
15 like everything else with FOIA, it can be rather gray.

16 Pardon me for one moment. I'd like to let  
17 John weigh in here.

18 MR. KROPF: I want to just supplement a  
19 little bit of what I'm hearing Bill answer on the B6  
20 question, which is obviously an important one for the  
21 Office. In a prior life, I was doing a fair number of  
22 FOIA cases for a different agency.

1           But really, the starting point for the B6  
2           is obviously the statute, and it starts with the  
3           statement that personal information would include  
4           things like medical files, personnel files, or similar  
5           files. There was a significant Supreme Court case in  
6           the early '80s, the Reporters Committee, which  
7           interpreted this statute, B6, and it created this --  
8           it was a multi-part test that talked about personal  
9           information and the balancing.

10           The first part of this test went to  
11           criteria 1, which is are we talking about personal  
12           information which fits into this category? And if the  
13           answer to that is yes, then the second part is asking  
14           the question what is -- what light are you shedding on  
15           the operations of government? In other words, what  
16           public interest would be served by disclosing the  
17           information? And you then continue the analysis by  
18           seeing the significance of the personal information,  
19           the significance of the operations, of the light it  
20           would shed on the operations of government, and then  
21           there's a balancing that goes on there.

22           And generally, that decision has sort of

1       been the touchstone for all of the B6 analysis.

2               I will say that in terms of guidance, the  
3       Department of Justice has an outstanding group of  
4       attorneys in their Office of Information Privacy who  
5       put out every two years a guidance, a compendium of  
6       all of the cases that will touch on all the  
7       exemptions, but Exemption 6 is one of those.

8               They will also do regular training on what  
9       the latest case law will say about what is  
10       disclosable, what isn't. I mean, generally, the  
11       presumption is overwhelmingly in favor of protecting  
12       that PII. If, as Bill said, it's a significantly high  
13       profile case that might shed light on the operations  
14       of government, then those are the rare cases, but they  
15       will look at the decision very closely and whether to  
16       disclose or not.

17              In addition to which -- I mean, the B6 also  
18       depends very heavily on the identity of the requester.  
19       If I'm writing in to get records about myself, then  
20       there isn't, obviously, the balancing analysis that  
21       you go through. But if I'm writing in to get records  
22       about Mr. Holzerland, then, of course, you have all of

1 the B6, the balancing considerations and so on. If he  
2 is, as a government servant -- I want to know about  
3 his personnel record, the chances of me finding  
4 anything out about that are extremely slim. I could  
5 say with great confidence I would get nothing. But  
6 the higher up you are in government, the higher  
7 profile that you have, the higher level of influence  
8 you might have on public government operations,  
9 actually the fewer privacy protections you might have.  
10 So the lower the government employee, more privacy  
11 protections. The higher, the fewer.

12 As I say, the Department of Justice, they  
13 really are the leaders in this area, and they do  
14 excellent training on it, and we'd be happy to provide  
15 you with materials that sort of explain the latest  
16 guidance in this area. There are even cases where  
17 even the most innocuous information might be protected  
18 that you wouldn't think of. For example, there was a  
19 Supreme Court case in the early '80s against the State  
20 Department to seek whether or not -- to know whether  
21 or not certain people had passport records, past  
22 passport records.

1           The analysis there was simply that we were  
2 not going to confirm or deny as the U.S. Government  
3 whether we even had those records on certain  
4 individuals because it might put them at risk. These  
5 particular individuals had to -- there was some  
6 question as to whether or not they were dual citizens  
7 of another country. And if it was known that they had  
8 U.S. passports, that could put them at risk.

9           So the analysis for privacy is one that's  
10 taken very seriously, and on the whole the presumption  
11 is that it's being protected in most cases. And I'm  
12 looking to Bill now to see if I've really over-stepped  
13 my time and bounds in anything I've said.

14           MR. HOLZERLAND: Not at all. No. Thank  
15 you, John.

16           MR. BEALES: Richard.

17           MR. PURCELL: One follow-up. And, John,  
18 thank you for bringing this up because my point is in  
19 a world where you have people who submit requests  
20 about themselves, and hopefully it's better -- a more  
21 well formed request than what do you know about me.  
22 But in any case, what are the criteria for

1 authenticating that the individual making the request  
2 is actually the individual who is the subject of the  
3 request?

4 MR. HOLZERLAND: Currently, one of the ways  
5 in which we do that is we require first-party  
6 requesters seeking information pertaining to  
7 themselves to either submit a notarized signature or a  
8 statement made under penalty of perjury that they  
9 essentially are who they say they are, and to provide  
10 us the bare minimum amount of identifying information  
11 possible that will allow us to confirm that they are  
12 the individual who is the subject of the record in  
13 question.

14 That's not always -- it's not always the  
15 easiest thing to do. For example, we may have -- if a  
16 requester named John Smith seeks records on  
17 themselves, we may find records on more than one John  
18 Smith. So we may have to go back to that requester  
19 several times to get additional pieces of identifying  
20 information to confirm, such as, for example, date of  
21 birth, city of birth, and these kind of things in  
22 order to confirm that they are, in fact, the correct

1 person. Requesters occasionally will provide  
2 voluntarily additional pieces of information. For  
3 example, though we don't solicit this, they may send  
4 us the last four digits of their Social Security  
5 number or their alien file number, or something else  
6 of that nature that will allow us to make sure we've  
7 sought and found the correct records and that we are  
8 releasing them to the correct party.

9 MR. PURCELL: My guess is the committee  
10 will ponder that for a moment, but it sounds  
11 insufficient in terms of modern society and the  
12 ability of people to impersonate one another based on  
13 the amount of information we all have about each  
14 other. I'm pretty sure I could probably put in a  
15 request for any person at the table here with  
16 sufficient information, including a notary that I paid  
17 for, to pass your test. But it doesn't actually mean  
18 that I've authenticated myself in a reasonably secure  
19 way.

20 It's a question I know we're all grappling  
21 with, and I'm not putting you on the spot too much  
22 here, Bill, but it's a policy issue that I'm concerned

1 about.

2 MR. HOLZERLAND: No, I'm glad -- I am glad  
3 that you brought this up because one of the things  
4 that we've been wrestling with for some time now is we  
5 are -- though I did not mention this during the  
6 presentation, we are drafting a Notice of Proposed  
7 Rulemaking to finalize our FOIA and Privacy Act  
8 regulations, and this is among the issues that we have  
9 wrestled greatly with, simply because the only way --  
10 for example, if you submit a request for records  
11 pertaining to yourself, the only way I'm going to  
12 guarantee that you are who you say you are would be if  
13 I know you personally or to knock on doors, or if the  
14 requester appears themselves to get the records and  
15 check photo identification or something of that  
16 nature, which would be incredibly inefficient.

17 So we're trying to find ways to use modern  
18 technology to facilitate the process and make it  
19 easier, and we're more than -- we'd be more than  
20 grateful for ideas on how we can do this in a more  
21 secure fashion to help us protect the personally  
22 identifiable information, and also to make the process

1 more efficient.

2           One of the things we wrestle with, even  
3 with the signature requirement, when you're sending in  
4 your Privacy Act request via snail mail, it may not  
5 get to the FOIA Office or the Privacy Act Office for  
6 some time because all of our mail, obviously, is  
7 screened. So there could be mail delays. So that  
8 does gum up the works in other ways, as well.

9           MR. BEALES: Have you looked at what credit  
10 reporting agencies do? I mean, they provide remote  
11 access to credit reports on an ongoing basis where  
12 there's obviously no physical identification or  
13 verification. It's a process that seems to work  
14 pretty well. It may depend on information that you  
15 don't have in your files because they know a lot about  
16 -- the credit reporting agency knows a lot about the  
17 real you that they can ask about. So it may not be  
18 something you can implement, but it's certainly a  
19 starting point on remote verification based on  
20 information rather than a physical credential.

21           MR. HOLZERLAND: Yes, that would make  
22 sense. Has it been among the ideas we've considered?

1 No, because, frankly, we don't -- as you mentioned, we  
2 don't know enough. We may not know enough about an  
3 individual where that would be feasible for us to do  
4 so. But again, we're willing and able to listen to  
5 any potential solutions to this quandary.

6 MR. HARPER: Howard, can I jump in on that  
7 point?

8 MR. BEALES: Sure.

9 MR. HARPER: Just to note the fact that you  
10 want to do some careful risk balancing here because if  
11 you do a too-careful inquiry into who you're dealing  
12 with, and you might share with them that you have no  
13 information or some very, very mundane information,  
14 you might end up doing more potential privacy harm in  
15 authenticating the person or identifying the person  
16 and ensuring that you're dealing with them than you're  
17 actually putting at risk any personally identifiable  
18 information.

19 So there are a lot of moving parts, and so  
20 you don't want to go in and do a deep dive on a  
21 requester when you're going to tell them, oh, and the  
22 answer is we don't have any information on you.

1           MR. HOLZERLAND: Well, that's a very good  
2 point. And also, beyond that, to conduct such a  
3 thorough inquiry, not only may the privacy harm  
4 outweigh the good, but it will also slow us down even  
5 further, and obviously that is not -- we're seeking to  
6 disclose the maximum amount of information in the most  
7 efficient manner possible. There's a little bit of  
8 tension there. Another thing we're working on.

9           MR. BEALES: I do think that looking at the  
10 credit reporting model might be useful. I certainly  
11 agree that you don't want to over-inquire. But the  
12 less -- where you have fairly little information about  
13 a person, you're not going to -- there's not going to  
14 be -- there's going to be less of a compromise of  
15 privacy if you mistakenly release it to somebody who  
16 is misrepresenting who they are. The more information  
17 you have, the more sensitive the information is, the  
18 more likely you'll be able to verify by using that  
19 information in a way that's better than just a  
20 signature.

21           MR. KROPF: One thing, if I might just  
22 mention, is we certainly recognize the incredible

1 expertise that's sitting before us on areas of  
2 authentication. One thing just to note from our side  
3 is I'm not sure how many tens of thousands of requests  
4 we're talking about here, but we have not had a  
5 problem yet noted with responding to requesters who --  
6 there just simply hasn't been a problem that's been  
7 brought to our attention in terms of the wrong people  
8 getting the wrong information.

9 MR. PURCELL: How would you know? If  
10 they're looking for information on somebody else,  
11 they're not going to come back to you and say, "Hey,  
12 thanks man, I just gamed you."

13 MR. KROPF: I'd just like to bring that  
14 fact to the committee's attention, with the tens of  
15 thousands of requests that we do process every year,  
16 that if somebody was playing that game to prove a  
17 point with us, maybe they would bring it to the press.  
18 But I'm not saying -- we don't know 100 percent. I'm  
19 just saying no one has mentioned it as a problem to  
20 us.

21 MR. HOLZERLAND: And to that end, I have to  
22 mention we did process -- this past fiscal year we

1 processed 109,000 requests and change, and that was  
2 not a complaint that we heard. But as you mentioned,  
3 if somebody is up to something nefarious, they're not  
4 going to come back and let us know. They're not going  
5 to send us a thank-you note.

6 MR. BEALES: Annie.

7 DR. ANTON: So I would just like to echo  
8 the concerns that I think we're hearing amongst the  
9 members. And first of all, all of the authenticators  
10 that you mentioned are a very weak form of  
11 authenticators. And so that's something that's of  
12 great concern to me. And in terms of not having heard  
13 anything yet about it being a problem, there are a lot  
14 of identity thefts and scams that take on where they  
15 hang on to that information for a while, and it may  
16 come back to haunt us in a bad way a few years down  
17 the road.

18 And so I'd like to really encourage the  
19 Office to actually actively pursue a better way, a  
20 more secure way, keeping in mind what Mr. Harper said  
21 about balancing risk, et cetera. But I think this is  
22 a very important area for focus.

1           MR. KROPF:  If I might just say that one  
2           suggestion is certainly the true experts and the true  
3           leaders for the FOIA program in the U.S. Government  
4           are the Department of Justice, and they've been doing  
5           this -- they've had an office that's been at this a  
6           very, very, very long time and have certainly looked  
7           at this issue before, and perhaps in talking to them  
8           we would get the benefit of their experience in the  
9           authentication issue.  That's something we could do.

10           MR. BEALES:  Tom Boyd.

11           MR. BOYD:  Thanks.  I just want to add my  
12           voice to those who have already spoken.  I mean, I  
13           agree with them with respect to the concerns that I  
14           think we all seem to share about how you validate that  
15           people are who they say they are.  And you indicated  
16           that, in response to Mr. Beale's question, that you  
17           have had some consideration given to the credit bureau  
18           model.  And some of us are more familiar than others  
19           with that model, but it's a very effective way of  
20           determining if you are who you say you are.

21                     Does that mean that you have met with  
22           representatives of that industry and tried to glean

1 from them methods by which you could be more effective  
2 in your assessment of identities, or just a general  
3 thought process about how to proceed?

4 MR. HOLZERLAND: To clarify my previous  
5 answer, we have not yet considered a model along the  
6 lines of what the credit bureaus are doing, but I  
7 agree that it is a -- clearly a more effective way of  
8 identifying -- guaranteeing that we're identifying the  
9 correct individual, and that it may be -- it may or  
10 may not be feasible for us to implement such a  
11 process, but that we would absolutely be willing to  
12 sit down and assess the feasibility of implementing  
13 such a process.

14 MR. BOYD: I would recommend that you  
15 consider at least sitting down with representatives of  
16 that industry, because you needn't divulge information  
17 in order to glean information if you know what  
18 questions to ask. And if it's questions -- if you're  
19 being asked to provide information by someone who  
20 purports to be the individual involved, then it should  
21 be relatively easy to determine by a Q&A process  
22 whether, indeed, that's the right person. And they

1 can help you a lot on that. I think it would be a  
2 useful thing to do. I think Mr. Beales is right.

3 MR. HOLZERLAND: And as John already  
4 mentioned, we are grateful for this committee sharing  
5 its expertise with us because we're clearly -- we're  
6 seeking all the answers, but we clearly don't have  
7 them. So this is one area that we're going to take a  
8 serious look at augmenting our current practices and  
9 enhancing them to make sure that we are identifying  
10 individuals appropriately and in an efficient manner.

11 MR. BEALES: We'll have all the answers  
12 when we're done with you.

13 [Laughter.]

14 MR. BEALES: John Sabo.

15 MR. SABO: Just a real quick data point.  
16 I'm assuming you accept electronic FOIA requests?

17 MR. HOLZERLAND: Yes, sir.

18 MR. SABO: Okay. So you have, in a sense,  
19 two categories, those who write in letters and those  
20 who submit electronic requests?

21 MR. HOLZERLAND: Yes.

22 MR. SABO: And in looking at the report, it

1 didn't seem to break those out, and that might be a  
2 good data point for the committee. In other words, in  
3 the electronic environment, you may need certain  
4 authentication controls that are distinct from the  
5 letter environment, and I don't see that broken out  
6 here, how many of the thousands you get are  
7 electronically submitted versus how many are submitted  
8 in letter. I think that would be a useful data point.

9           The second thing would be -- so that's one  
10 question, if you could provide that. And the second  
11 request would be do you have trend data over the last  
12 X years of the life of the FOIA Office over how your  
13 processing is going in terms of those electronically  
14 submitted? Are you improving your processing time?

15           You've got average pendings here of 300  
16 days or so in many of these agencies, components, and  
17 those are pretty long but probably similar to other  
18 agencies. So how are you doing in improving in those  
19 two categories? I wonder if you have data along those  
20 lines.

21           MR. HOLZERLAND: To address the first  
22 portion of your question with respect to the breakout

1 of how -- what percentage of requests are submitted  
2 via different methods, that's not one thing -- that  
3 one piece is not something we have been required to  
4 report upon in our annual report to the Attorney  
5 General. However, we do -- at least the bulk of DHS  
6 FOIA offices, but definitely the Privacy Office, we do  
7 track internally how requests are submitted.

8           Obviously, we treat them all equally  
9 whether it's email, fax, or mail, or any other method.  
10 But that's not something that we've been required to  
11 report upon, but that is an excellent suggestion.  
12 That's something that perhaps we could take a closer  
13 look at internally. We might find that information  
14 very, very helpful.

15           As far as the processing goes, are you --  
16 if you could clarify that.

17           MR. SABO: The question is on trend data.  
18 Agencies like Social Security, which are very workload  
19 based, track over courses of years are they improving  
20 or is their processing time decreasing, or is the  
21 processing time stagnant, or is it improving, and by  
22 what degree? In the report, there are no charts at

1 all. It's columns of data, and in contemporary  
2 reporting you often use visual graphics to say, okay,  
3 this is what percentage, and you can visualize it.

4 So I'm wondering on a longitudinal basis  
5 how the Office is doing in processing. Are your  
6 pendings down? Are your processing times decreasing  
7 year after year?

8 MR. HOLZERLAND: Well, that's one of those  
9 things that we do track. We keep a close eye on all  
10 of these areas internally. Currently, we recently --  
11 well, we recently wrapped up an audit. GAO has  
12 visited with DHS and probed extensively into the FOIA  
13 program, and a report will be issued. I believe it's  
14 scheduled to be issued during Sunshine Week, which is  
15 mid-March, I believe the second or third week of  
16 March.

17 That will provide, I think, a little bit  
18 closer look at how we've performed over time. For  
19 example, we can say -- I can say with certainty that  
20 if I take two given points in time, say mid-September  
21 of 2006 versus mid-October 2008, I can tell you that  
22 our pending requests were down by about approximately

1 35,000 and change. But more importantly, our backlog  
2 was down 24,000 and change.

3           So we've decreased the backlog. We  
4 processed more requests than we received last year. I  
5 think we received just over 108,000. We processed  
6 over 109,000. You may notice that the cost of the  
7 program, if you look at, say, '06 versus '08, it was a  
8 little bit less as well. So we're trying to do more  
9 with less, process more requests faster and that sort  
10 of thing.

11           To that -- in order to do these, to achieve  
12 a reduction in backlog, we have -- I mentioned the  
13 FOIA Improvement Plan. We have set goals and  
14 milestones for all of the components with existing  
15 FOIA backlogs that they were required to meet and  
16 report to us on.

17           So as a follow-up, the Deputy Chief FOIA  
18 Officer and myself visited each and every FOIA office  
19 in the Department last year at this time. We didn't  
20 conduct an audit but we took a good, hard look at  
21 their business practices, their processes, procedures,  
22 at their files, and made suggestions, suggested some

1 improvements that could be made in order to meet the  
2 goal, which is a zero backlog, of course.

3 MR. BEALES: Jim Harper.

4 MR. HARPER: Thanks. I wanted to return  
5 briefly -- I thought I had sent Kirk Herath from the  
6 room by threatening to ask more questions, but he's  
7 evidently returned. I'm sorry, Kirk.

8 But I wanted to return briefly to the  
9 question of the credit bureau model, and we're going  
10 to have a conversation about it with you here. So  
11 pretend like it's a question addressed to you, but it  
12 isn't necessarily. I actually wanted to get more  
13 clarification from my colleagues, what you mean by the  
14 credit bureau model, because there are a couple of  
15 different things you might mean by that, and I want to  
16 know what it is that you're suggesting.

17 MR. BEALES: Well, my microphone seems to  
18 have died, so I'm just going to talk loudly. What I  
19 had in mind with the credit bureau model --

20 COURT REPORTER: I'm sorry to interrupt  
21 you. [Inaudible.]

22 MR. BEALES: It's good that this committee

1 is so rich in expertise.

2           What I had in mind with the credit  
3 reporting model is when you try to get a credit report  
4 online, they will ask for a -- they will ask a series  
5 of questions. It's not a stable set of questions.  
6 It's a variable set of questions, because if it was  
7 stable, people could figure out the answers and come  
8 back again. They are referred to as out-of-wallet  
9 questions.

10           They also sell this kind of authentication  
11 service to commercial clients who can use it, use the  
12 same sorts of questions to get some verification that  
13 this really is the person.

14           And the idea of all of these things is they  
15 know the information from your credit report. You  
16 know the information because it's in your wallet. And  
17 hopefully the thief doesn't have your wallet. It's  
18 not perfect, but it is considerably better than  
19 signing your name.

20           MS. McNABB: Actually, I think the out-of-  
21 wallet expression means something slightly different  
22 from that. The questions that they ask you, that the

1 credit bureaus ask you is information that they have  
2 in their files on you that is not in your wallet. So  
3 it's less available to outsiders.

4 So the analogy would be for DHS is to ask  
5 questions based on information they have in their  
6 files that is not more generally available. I'm  
7 hoping that we do not mean to be recommending buying  
8 the credit bureau product, authentication product  
9 based on the credit bureau data. Is that what you --

10 MR. BEALES: No. I mean, Jim's point is  
11 good. Unless you've got a whole lot of information  
12 about somebody, that's probably not worth it. That  
13 doesn't make a lot of sense. And I don't know, but  
14 the idea of using the information you have to try to  
15 figure out whether this is the person who should be  
16 able to get this information, that seems worth  
17 exploring.

18 Now, if all you know is that they're on a  
19 watch list, you can't very well ask them which watch  
20 list are you on. So, you know, it may not work as  
21 well in this context as it does in others.

22 MS. McNABB: It could be passport data. It

1       could be border data. It could be things like when  
2       did you last travel outside of the country? Where did  
3       you go? I mean, it could be, depending on what kind  
4       of records you're looking for. It could be an  
5       analogy.

6               MR. BEALES: In some cases, it may be a lot  
7       of information. That's right, that's right, depending  
8       on who it is and what it is.

9               MR. HARPER: That's a helpful  
10       clarification, because I see there being two different  
11       possible credit bureau models. One is going to credit  
12       bureaus and asking them to provide identity proof  
13       services and that kind of thing, and that's -- well,  
14       there's a version of that that goes on if you show up  
15       at the airport without an I.D. card, and they dig into  
16       not necessarily credit bureaus but they dig into a  
17       deep well of data about you that isn't necessarily  
18       cool.

19               If you're looking for shared information,  
20       that is information that both parties know and others  
21       generally wouldn't know, that seems like an  
22       appropriate thing. I guess I take it that that's what

1 you were referring to.

2 MR. BEALES: That was the model I was  
3 referring to, yes.

4 MR. HARPER: Okay. In my book I refer to  
5 that as epistometric identification. That is based on  
6 what you know, as opposed to biometrics. The book is  
7 for sale on Amazon.com.

8 [Laughter.]

9 MR. BEALES: Okay, Joanne. Did you have a  
10 question?

11 MS. McNABB: Just one quick question. The  
12 other point I was making was just that point. We do  
13 not mean to be recommending talking to credit bureaus  
14 about their authentication products but about an  
15 analogous process.

16 My other question is of the 108,000 or  
17 109,000 requests you either received or processed last  
18 year, how many of them or what percentage of them were  
19 first-party or Privacy Act requests?

20 MR. HOLZERLAND: I'd have to examine the  
21 annual report to give you exact figures. But I can  
22 say that of the -- the component that received the

1 greatest amount of requests, which would be U.S.  
2 Citizenship and Immigration Services, they received  
3 just under 79,000 requests. Of those, there's a very  
4 small percentage that's for -- that were not first-  
5 party requests for access.

6 MS. McNABB: So a lot of that 109,000 were  
7 first party.

8 MR. HOLZERLAND: Correct.

9 MS. McNABB: Okay. Thanks. And I can find  
10 it.

11 MR. BEALES: Lance Hoffman, last question.

12 MR. LANCE HOFFMAN: Okay. Thank you, Mr.  
13 Chairman. I have not seen such an animated discussion  
14 of FOIA in a long time.

15 MR. HOLZERLAND: I'm excited. Very  
16 pleased.

17 MR. LANCE HOFFMAN: This is -- this  
18 actually -- I don't want to steal Jim Harper's  
19 thunder, but I know there was some discussion in the  
20 Privacy Architecture Subcommittee meeting about  
21 considering recommending a workshop on topics of  
22 interest, of which this may clearly be one. But we

1 can perhaps revisit that later.

2           You did mention about, I guess, 15 minutes  
3 ago now that it would be clearly more effective -- I  
4 think those were your words -- to use the credit  
5 bureau model, whatever that is. I'm not convinced.  
6 It may be more efficient. It may not be more  
7 effective for all the reasons that have been stated  
8 earlier.

9           So I would just urge you to -- this is a  
10 complex area, merging identification, authentication,  
11 and the tension between giving out information and  
12 privacy, and I think it may be more appropriate to  
13 both, as you said, go to see what DOJ has done, but  
14 also to see what others have done and look at it,  
15 whether it's in a workshop or some other way, and then  
16 you can have a reasonable -- a more reasonable answer.

17           I think you should be commended for being  
18 willing to look at this proactively because I agree  
19 with what Richard said, Richard Purcell, that just  
20 because you haven't been told that you've been had  
21 doesn't mean you haven't been had.

22           On the other hand, that doesn't mean that

1 you should go and do a lot of stuff to prevent that.

2 It's a cost/benefit question.

3 MR. KROPF: Thank you for that, Lance. And  
4 I just want to -- I do want to be very clear about  
5 this. It is, obviously, a very valid concern, and we  
6 certainly appreciate the committee's attention and  
7 expertise on this. But the thing I also want to be  
8 very clear about is, with all the caveats that you've  
9 mentioned, there has not been a problem reported to  
10 us. So I want the record to be very clear that this  
11 is not the subject of a current controversy or a  
12 reported problem. Certainly a valid concern,  
13 certainly something that bears looking at.

14 Again, I think for us internally, probably  
15 the best thing to do is consult with those that have a  
16 government-wide perspective that can see the big  
17 picture of how FOIA is processed across all the  
18 government agencies, and that would be those leaders  
19 like the Department of Justice and OMB. And it might  
20 be something worth our time to explore with them.

21 Bill, is there anything you want to add?

22 MR. HOLZERLAND: No, I think you summed it

1 up pretty nicely. We do recognize, particularly in  
2 our Office, that privacy and transparency are two  
3 sides to the same coin, and there's always the tension  
4 of how can we be sure we're protecting personally  
5 identifiable information of individuals, but at the  
6 same time releasing the maximum amount of information  
7 we're able to.

8           So we do recognize that there's a tension  
9 there and there's not always these clear cut and dried  
10 answers. But we are, as you said, proactively looking  
11 to solve some of these sort of issues, and again I  
12 want to thank the committee for taking the time to  
13 share its views on this particular subject with us.

14           MR. BEALES: All right. Thank you, Mr.  
15 Holzerland. Thank you, John, for being with us.

16           We will now break for lunch. We do not  
17 have an administrative session. There will be a  
18 couple of emails from Martha on what are essentially  
19 administrative matters, but we can do it that way  
20 rather than trying to kick everybody out and wait for  
21 the room to turn over.

22           We are on our own for lunch. I have a

1 couple of copies of the menu from the hotel, if  
2 anybody is interested in exploring that possibility.  
3 But otherwise, we are on our own.

4 Please be back so that we can start  
5 promptly at 1:30 because we have a speaker with  
6 schedule constraints. So if we could get started  
7 promptly at 1:30, that would be excellent.

8 Thank you, and we will see you this  
9 afternoon.

10 [Lunch recess at 12:39 p.m.]

11

12

13

14

15

16

17

18

19

20

21

22



1 has been a director since December of 2005, and he's  
2 been the managing agent for the Travelers Redress  
3 Inquiry Program, otherwise known as TRIP, since its  
4 launch in February of 2007.

5 Mr. Kennedy has also served in several  
6 other capacities at TSA, including acting deputy  
7 assistant administrator for compliance programs and  
8 program manager in the Office of Information  
9 Technology.

10 Welcome, Mr. Kennedy, and I'm sure we'll  
11 have questions.

12

13

14

15

16

17

18

19

20

21

22

1 TRAVELER RELATED REDRESS PROGRAMS AT DHS

2 MR. KENNEDY: I'm sure you will. Thank you  
3 very much, Mr. Chairman, and members of the committee.  
4 Good afternoon. I would like to take the opportunity  
5 to thank you for allowing me to come in and to discuss  
6 traveler-related redress at the Department of Homeland  
7 Security.

8 As some of you may know, I previously  
9 addressed this committee in December of 2005 and  
10 September of 2006. When I last appeared before the  
11 committee, my focus was entirely on redress efforts at  
12 the Transportation Security Administration, TSA, as a  
13 director of the Office of Transportation Security  
14 Redress. Since that time, the mission of OTSR has  
15 expanded to include additional responsibilities as a  
16 designated lead agent for DHS TRIP, as you mentioned,  
17 and as a designated DHS officer for Office of Appeals  
18 and Redress.

19 Today I actually come forward to discuss  
20 traveler-related redress efforts across DHS. If you  
21 would please allow me to briefly highlight some of the  
22 changes that have taken place since my last appearance

1 before the committee, hopefully I'll answer some of  
2 your questions before you have a chance to ask them.

3 In January of 2006, then-Secretary of DHS  
4 Chertoff, and then-Secretary of State Rice, announced  
5 a joint vision for secure borders and open doors, also  
6 known as the Rice-Chertoff Initiative. Part of this  
7 vision included the creation of a government-wide  
8 redress program to enable travelers to resolve  
9 screening complaints through a single office. The  
10 outcome of this vision became known as DHS TRIP.

11 In October of that same year, after  
12 reviewing the redress capabilities within the  
13 Department, the DHS TRIP governance board determined  
14 that TSA OTSR was best suited to lead the Department's  
15 redress efforts in support of the Rice-Chertoff  
16 Initiative.

17 Subsequently, then-Secretary Chertoff  
18 designated OTSR as the lead agent for DHS TRIP. In  
19 February of 2007, DHS TRIP was launched as a central  
20 processing point for redressing complaints from  
21 travelers who were either delayed or denied boarding  
22 on commercial air carriers that operated within United

1 States air space; entry into the United States via  
2 airport, seaport, or border crossing; or from  
3 individuals who were repeatedly subjected to  
4 additional screening.

5 The DHS TRIP program office is responsible  
6 for managing the process for intake, inquiry review,  
7 and determination, as well as the response to the  
8 applicant. This is indeed a big responsibility but is  
9 not one that the program office shoulders alone. DHS  
10 TRIP actually works with DHS headquarters offices such  
11 as the Screening Coordination Office, Privacy Office,  
12 the Office of Civil Rights and Civil Liberties, and US  
13 VISIT. We also work with other components, including  
14 TSA, Customs and Border Protection, Customs and  
15 Immigration Services, and Immigration and Customs  
16 Enforcement.

17 We also work with other government  
18 representatives such as the Department of State  
19 through their Bureau of Consular Affairs and their  
20 Passport and Visa Offices, as well as Department of  
21 Justice through the Terrorist Screening Center to  
22 review and make a determination regarding the status

1 of every traveler who applies for redress via DHS  
2 TRIP.

3           Shortly after the launch of TRIP, TSA and  
4 DHS briefed Congress, as well as the 9/11 Commission  
5 on TRIP. While both the Commission and Congress liked  
6 the idea of one-stop shopping for traveler-related  
7 redress, especially for airline passengers, they  
8 wanted to formalize the responsibility of redress at  
9 DHS TRIP. With this in mind, Congress included  
10 Section 1606, Appeal and Redress Process for  
11 Passengers Wrongly Denied or Prohibited from Boarding  
12 a Flight, in the 9/11 Act.

13           On August 6, 2007, the 9/11 Act was signed  
14 into law. To comply with the Act's redress mandate,  
15 then-Secretary Chertoff designated OTSR as a DHS  
16 office of appeals and redress on December 10, 2007.

17           While it is nice to talk about how  
18 traveler-related redress has evolved at DHS, many are  
19 wondering how to participate. Information about the  
20 program can be found in hard copy at border crossing  
21 stations and at airports, electronically at the DHS  
22 screening components' websites, or by calling or

1 emailing the TSA Contact Center.

2           The process for submitting a redress  
3 request is actually fairly simple. Anyone who feels  
4 that they were inappropriately denied travel due to  
5 the Department's screening procedures is invited to  
6 submit a travel inquiry form to DHS TRIP. One may  
7 submit a request electronically through the DHS TRIP  
8 website, which is [www.dhs.gov/trip](http://www.dhs.gov/trip). One may also  
9 request a hard copy of the form by calling a TSA  
10 contact center. And in order to address privacy  
11 concerns related to providing personally identifiable  
12 information to the government, DHS TRIP actually  
13 accepts inquiries with the minimum amount of PII  
14 required for processing.

15           DHS TRIP asks travelers to identify their  
16 areas of concern up front in order to determine what  
17 documents are required for processing. For electronic  
18 submissions, this is actually done by creating a  
19 unique smart form that automatically requests the  
20 minimum amount of personal information that is  
21 required. For those submitting paper forms, Section 5  
22 of the TIF instructs the traveler on what is required.

1 For those needing additional information, the TSA  
2 Contact Center, as well as the TRIP Program Office,  
3 are always available to assist.

4 When we receive a redress inquiry, we check  
5 to ensure that we have all the documents that are  
6 needed to process the request. Once we confirm that  
7 the inquiry is complete, we work with our stakeholder  
8 organizations, as well as other government agencies  
9 including law enforcement and intelligence  
10 organizations, to confirm the applicant's identity,  
11 determine if the individual is a person of interest to  
12 the Federal government, and if so, to ensure that the  
13 individual is associated with the appropriate watch  
14 list.

15 Once the review is complete, we issue a  
16 determination letter to the applicant, and we also  
17 work to clarify that person's status with DHS TRIP --  
18 with DHS stakeholders. In other words, if the  
19 applicant has been misidentified as a person who is on  
20 a watch list, we give stakeholders such as the airline  
21 operators additional personal information in order to  
22 quickly confirm a request for his identity.

1           As you can imagine, DHS TRIP is really  
2 extremely busy. Since the launch of the program, over  
3 51,000 individuals have applied for redress under DHS  
4 TRIP. During our busy season, which is during the  
5 summer and holiday travel seasons, we receive on  
6 average almost 1,000 cases per week.

7           DHS TRIP has adjudicated and closed over  
8 30,000 redress requests. Approximately 16,000 cases  
9 are pending additional information from the applicant  
10 before we can move forward, while we have currently  
11 approximately 5,000 requests under review.

12           While I'm proud of our accomplishments thus  
13 far, we still have plenty of work to do. Our  
14 statistics show that the number-one area of concern  
15 for redress requesters is air travel, at 65 percent,  
16 while border crossings are coming in second at 16  
17 percent. Our analysis shows that 99 percent of  
18 redress requests related to aviation do, in fact,  
19 involve cases of misidentification.

20           DHS and TSA have taken steps to reduce the  
21 number of misidentifications associated with airline  
22 travel. In April of 2008, then-Secretary Chertoff and

1       then-Assistant Secretary Hawley reminded the  
2       commercial airlines that they do, in fact, have the  
3       responsibility to securely store a traveler's name and  
4       date of birth, if requested, in order to avoid future  
5       cases of misidentification.  Additionally, just last  
6       month, TSA began the rollout of the Secure Flight  
7       Passenger Pre-Screening Program.  Secure Flight  
8       transfers the responsibility for watch list pre-  
9       screening to the government in an effort to reduce the  
10      instances of misidentification.

11                 Lastly, DHS TRIP has partnered with Secure  
12      Flight and will continue to offer traveler-related  
13      redress for those who believe that they are  
14      inappropriately delayed or denied air travel.

15                 DHS TRIP is also looking for additional  
16      ways to increase the efficiency and effectiveness of  
17      the program while at the same time safeguarding the  
18      privacy of the traveling public.  DHS TRIP is  
19      currently looking at upgrading its case management  
20      system in order to reduce the potential for mistakes  
21      and to reduce processing times.

22                 We look forward to continuing to work not

1       only with this committee but the privacy community at  
2       large to help TSA accomplish our goal of protecting  
3       our country while defending our freedoms.

4               I look forward to answering any questions  
5       that you may have at this time.

6               MR. BEALES: Thank you very much.

7               John Sabo.

8               MR. SABO: Thanks very much. Just a quick  
9       couple of questions that don't seem to be in the  
10      slides. Do you have follow-up with the resolved cases  
11      to determine if the individuals are satisfied with the  
12      result or with the process? And secondly, do you have  
13      data on how many of the users of this TRIP system are  
14      repeat users, where they have to come back multiple  
15      times?

16              MR. KENNEDY: Well, what we do have is we  
17      do have people that, once they go through the process,  
18      they actually do come back and they say, well, this is  
19      what happened to me afterwards. Let's say that the  
20      person was an aviation -- a traveler, traveled on an  
21      airline, and they said, "Hey, I went through this  
22      process, and I still have had trouble."

1           And so what we do in those instances, we  
2       find out specifically what happened and we actually go  
3       back to the air carrier through our security  
4       inspectors at TSA in order to find out what happened  
5       and why. If a person continues to have problems, then  
6       what we do is, like I said, we work with that air  
7       carrier so that they recognize that the person  
8       actually has gone through the cleared process and to  
9       help that person down the road.

10           And when we have cases of misidentification  
11       with CBP, we also work with CBP and we make sure that  
12       the systems are up to date so that that individual  
13       will be able to go through with a moderate amount of  
14       delay.

15           As for additional statistics, that's one of  
16       the reasons why we want to actually update the case  
17       management system, because we do not collect those  
18       statistics right now. When we started, we wanted to  
19       make sure that we actually got this started, one-stop  
20       redress started across the Department. But as you can  
21       kind of imagine, as we go forward, as we had the  
22       opportunity to go forward, we've actually learned

1 different things. So we want to actually upgrade the  
2 system so we can keep those statistics and also be  
3 able to communicate with the stakeholders when we see  
4 there's an issue.

5 MR. SABO: I mean, just a quick follow-up.  
6 So processing times, obviously, are going to vary  
7 depending on the nature of the complaint. But do you  
8 have any statistics on average processing time, or --  
9 because anecdotally what's happening is you see  
10 occasionally on television programs some very  
11 egregious example of somebody who has been denied  
12 boarding and it makes the national news, but it may  
13 not reflect the steps you've taken to resolve issues.  
14 And that's why I'm looking for some data on --  
15 statistical data on processing times and so on.

16 MR. KENNEDY: Processing time, obviously,  
17 since we launched DHS TRIP, because of the fact that  
18 we're not just dealing with one specific area, we're  
19 dealing with multiple areas, and like I said, we do  
20 have -- most of the ones are TSA only. But a lot of  
21 them actually do cross the spectrum. And when we have  
22 those that cross the spectrum, there are times they

1 could take 60 or 70 days to resolve the issue. But  
2 what we're doing is we're actually resolving the issue  
3 across the board.

4 In cases where -- that's an average.  
5 Sometimes it's much, much less. And obviously, when  
6 we were just TSA and we were dealing with one issue,  
7 there were times when we were down to about 10 days  
8 because it was a fairly simple process.

9 But now, with the complexities that are  
10 involved, we actually are a little bit longer. But  
11 one of the things in which we know that the case  
12 management system will do is we actually have cases  
13 now where, because of the fact that we have -- we do  
14 have an automated system, but we do have cases where  
15 we still have manual processes, and those actually  
16 slow down the process.

17 And so with the case management system,  
18 what we will be doing is actually reducing the amount  
19 of manual intervention that's necessary so we can  
20 actually go forward again in a fairly quick manner.

21 MR. BEALES: Kirk.

22 MR. HERATH: I think, John, I had some of

1 the same concerns. You answered some of my questions.  
2 So we talk about here that 30,000 cases have been  
3 adjudicated and closed, and I think, similar to John's  
4 question -- so by closed, do we mean resolved?

5 MR. KENNEDY: We mean resolved.

6 MR. HERATH: And do we mean resolved, you  
7 know, favorably in the complainant's -- so do you have  
8 statistics on how many people still have -- are still  
9 on lists, how many people still have an unresolved, in  
10 their minds, problem?

11 MR. KENNEDY: Well, like I said, when we  
12 say it's resolved, we know that the person is -- we  
13 adjudicated it correctly. There are some that, as I  
14 mentioned before -- a number of them, the overwhelming  
15 number of aviation cases are misidentified, and we are  
16 able to actually work with the airlines.

17 But we actually do have a number that is  
18 not a misidentification, and what we do is we go back  
19 and we work with not only the Terrorist Screening  
20 Center but the nominating agency to make sure that the  
21 information which the listing, the Federal Watch List  
22 listing is actually still valid and still correct. If

1 it is, then we make sure the person is appropriately  
2 watch listed. If not, then we take steps to change.

3 Now, if you're asking me today how many  
4 people exactly are on the cleared list, I can't tell  
5 you that because that's actually a matter of national  
6 security. But what I can tell you is one of the  
7 things that people have gone around saying, and we've  
8 actually seen where people have said, "Oh, there's  
9 over a million people who are actually on the watch  
10 list."

11 One of the things that then-Secretary  
12 Chertoff actually said back in October of 2008, he  
13 actually gave some statistics where the number of  
14 individual persons on the consolidated watch list was  
15 about 400 -- a little bit under 400,000. And we have,  
16 for TSA, when you look at aviation, selectee and no  
17 fly, you have a much smaller number. That's a much  
18 smaller subset, obviously, of that list. So you've  
19 got less than 17,000.

20 But the most important thing that you look  
21 at are the fact that -- are the people appropriately  
22 watch listed. My process is the one where we actually

1 go through and we make sure on each and every case  
2 that the person is appropriately watch listed.

3 MR. HERATH: And I can't recall, but do you  
4 have a timely review requirement? Is there -- is  
5 there -- so, part of due process is obviously to get a  
6 hearing, but the second wing of that would be that  
7 it's timely and that they don't -- they're not in some  
8 sort of vortex.

9 MR. KENNEDY: We do not have a set date set  
10 in stone that says you must complete this review in X  
11 amount of days. What we do is, in our case, we want  
12 to make sure that we get it right. So instead of  
13 going through and just giving the person an answer, we  
14 actually go through and make sure that the entire  
15 process is complete and that the person actually does  
16 receive redress.

17 There are cases where it will take a lot  
18 longer depending on the issue, because not only do we  
19 deal with U.S. persons, but we deal with any traveler  
20 who has attempted to travel to the United States,  
21 including foreign citizens.

22 MR. HERATH: And one final -- one final

1 question. So from your office, what's the appeal  
2 route?

3 MR. KENNEDY: Pardon me?

4 MR. HERATH: From your office, what is the  
5 appeal route to a person who doesn't feel like they've  
6 been adjudicated properly?

7 MR. KENNEDY: It depends on the nature of  
8 the complaint. If it's an aviation-related complaint,  
9 if the person is not satisfied, and we actually spell  
10 this out when we actually send them a determination  
11 letter, they actually are able to appeal to the U.S.  
12 Court of Appeals.

13 If it's a case where it is clearly a no-fly  
14 case, they are actually given instructions on how to  
15 apply for a final agency decision, which in that case  
16 would be the assistant secretary for TSA. And if that  
17 person didn't like that final agency decision, they  
18 can go on to the U.S. Court of Appeals.

19 Others would be going basically straight to  
20 District Court.

21 MR. HERATH: Okay. Thank you.

22 MR. BEALES: When somebody goes through the

1 process and it's not a misidentification, what exactly  
2 are they told in the determination letter?

3 MR. KENNEDY: The determination letter,  
4 because of the fact that in many cases we -- well,  
5 right now I cannot tell somebody individually if they  
6 are or are not on the watch list. That is -- the  
7 Attorney General actually had a finding of fact that  
8 the information -- the individual names on the watch  
9 list is, in fact, a state secret. So I cannot sit up  
10 here and tell them that.

11 What they are told is the fact that we have  
12 closed the case. When we have actually updated the  
13 records, as appropriate, we've actually said this is  
14 for individuals who the next time that they travel, to  
15 make sure that they actually contact their air carrier  
16 to be able to -- and we offer the fact that the air  
17 carrier can, in fact, store their name and their date  
18 of birth so that there will be less cases of -- less  
19 of an issue when the person actually goes to the  
20 airport.

21 For those that are traveling across the  
22 border, if there's an issue, we encourage them to

1 speak with the supervisor. But we never tell --  
2 unfortunately, I'm not in a position to be able to  
3 tell them you are or you are not. That's just not  
4 something I can do. But what I can do is give them as  
5 much information as I can about making sure that they  
6 clarify their identity.

7 MR. BEALES: And if -- for somebody who is  
8 on the list, I mean, it doesn't sound like -- and that  
9 you think is properly on the list, it doesn't sound  
10 like it's going to help much to give the airline my  
11 name and date of birth. I mean, that's a guarantee.

12 MR. KENNEDY: What it will do is,  
13 basically, if you are on the watch list -- and one of  
14 the things we want to do is we want to make sure that  
15 you are not misidentified. But if you are, we want to  
16 make sure that you know that, hey, look, we did review  
17 this case, you did go through the process, we did make  
18 sure that the appropriate steps were taken. But in  
19 the case of actually discussing something with the  
20 airlines, hey, at least the airline knows exactly who  
21 you are so you can get the proper screening so you can  
22 be on your way.

1           MR. BEALES: Could I just ask one more  
2 question before I go back to the rest of my  
3 colleagues? You mentioned that in the aviation cases,  
4 99 percent of the inquiries are, in fact,  
5 misidentification. Do you know what that is in the  
6 other cases, in the CBP or --

7           MR. KENNEDY: Land border?

8           MR. BEALES: Yeah.

9           MR. KENNEDY: It's a lot less. I don't  
10 have the exact statistics with me right now. But the  
11 cases of misidentification are actually a lot less.  
12 The issues that we have with CBP is when a person is  
13 actually being interviewed by a border patrol officer,  
14 there are many things that that border patrol officer  
15 is actually screening for, not just terrorism-related  
16 cases.

17                   So it could be an actual person who is a  
18 threat, but the person may not be a terrorism threat.  
19 They may be criminal. It may be a criminal case.  
20 That person could be wanted for murder or something  
21 like that, or some other type of offense. So the  
22 cases are a lot less -- there's a lot less -- the

1 percentage is a lot less for misidentifications.

2 But like I said, because of the fact that  
3 you have such a wide range, that's -- like I said, I  
4 don't have the exact statistics, but there are other  
5 reasons why the person would be stopped at the border.

6 MR. BEALES: All right. Thank you.

7 Lance Hoffman.

8 MR. LANCE HOFFMAN: Thank you. Two  
9 questions. First of all, I noticed in your slides  
10 that you say approximately 16,000 requests are  
11 awaiting submission of supporting documentation --

12 MR. KENNEDY: Correct.

13 MR. LANCE HOFFMAN: -- from the traveler,  
14 such as the required Privacy Act notice statement and  
15 copies of identification documents. I'd like to know  
16 if you could explain just a bit more. What is this --  
17 the required Privacy Act notice statement. Is there  
18 something missing they've been asked for and they  
19 haven't produced related to that statement?

20 MR. KENNEDY: Well, on the Privacy Act  
21 statement, we actually have two things, the Privacy  
22 Act statement, as well as the Penalty of Perjury

1 statement that an individual must sign to acknowledge  
2 the penalty of perjury before we can actually proceed.

3           The other thing is, for the identity  
4 documents, what we need to be able to do is if a  
5 person has an issue and they have the area of concern,  
6 and it is a -- it leads us to believe this is a border  
7 crossing issue, if someone gives us, let's say, a  
8 driver's license, we can't do anything with that  
9 because it's a border crossing issue. So we need to  
10 have -- and that's what we make clear up front. But a  
11 lot of times people will submit the wrong documents.

12           So what we have to do is we have to hold  
13 that until we get the correct documents. And one of  
14 the things in the updated case management system that  
15 we're going to be doing is saying, well, okay, we're  
16 going to put a time limit on the amount of time that  
17 you can actually respond, just like we did in the  
18 beginning, which was about 45 days, and if you don't  
19 respond within that time, then we will  
20 administratively close it just so it doesn't hang open  
21 like that.

22           MR. LANCE HOFFMAN: Well, I thank you for

1 leading me to my second question, which is about the  
2 case management system. I don't know if you've shared  
3 information before with this committee or not on it,  
4 but if you haven't, it would be interesting seeing  
5 something on it.

6 Really, when is it going to be up and  
7 running?

8 MR. KENNEDY: We actually have a -- now we  
9 have a system. What we're talking about is an upgrade  
10 to the existing system. There is an actual IT system  
11 in place right now. As a matter of fact, that is how  
12 the public communicates with us. What we're talking  
13 about doing when we upgrade the case management  
14 system, instead of us individually having to deal with  
15 a number of different systems, basically taking  
16 information out of one system and putting it in  
17 another, we will actually be able to do that  
18 automatically.

19 So right now there's a case management  
20 system. Right now there is a -- it's more of a  
21 custom-based case management system, and we're going  
22 to more of a COTS or off-the-shelf system where you

1 configure it versus customize it, and it's going to be  
2 -- and the reason why we're doing that, number one,  
3 changes are a lot less expensive for us to make, and  
4 as technology improves, we can take advantage of the  
5 emerging technology, and we can actually do less human  
6 intervention. Those are the types of things that  
7 we're talking about.

8 MR. LANCE HOFFMAN: So when is the upgrade  
9 going to be implemented across the agencies and up and  
10 running?

11 MR. KENNEDY: That is something that right  
12 now we're still in the procurement process. What we  
13 are actually -- we actually have gone through  
14 requirements right now. We've actually talked with  
15 all of the different stakeholders across the  
16 Department, as well as DHS, as well as -- excuse me --  
17 Department of State, as well as the Department of  
18 Justice. So we've actually gone through the  
19 requirement standpoint.

20 What we actually have to do is go through  
21 the government procurement process, which is not  
22 something that I can do in 30 days. So it is

1 something that does take time. But we are actually  
2 hoping to have that in place before, at some point,  
3 the initial piece, because it's really spiraling  
4 development. You will start a central case, and as  
5 you look at additional features, you will actually add  
6 additional pieces to it.

7 But we actually hope to have the central  
8 case management system in place before we're actually  
9 through 2010.

10 MR. BEALES: Jim Harper.

11 MR. HARPER: Thanks. Thanks. Thanks for  
12 coming back. Nice to see you again. You're a  
13 regular.

14 [Laughter.]

15 MR. HARPER: I was gratified to hear my  
16 colleague, Kirk Herath, speak in terms of due process,  
17 because that's what redress is, is generally  
18 Constitutional due process. And there was a case in  
19 the Ninth Circuit recently. I don't know if Martha  
20 passed it along to you, but I sent it to her. Whether  
21 or not you're familiar with it, it's important because  
22 it established a placement on a list that causes a

1 person to receive derogatory treatment is a due  
2 process violation, if there isn't a means to get them  
3 off such a list.

4           The Ninth Circuit's case was perhaps more  
5 compelling than a transportation security case because  
6 this was a set of parents who were entirely innocent  
7 but they were placed on a child molesters list or  
8 something like this. So it was a really, really  
9 horrible case. But I think it established the  
10 important point that we're talking about, due process.

11           If people are on a list -- now, in this  
12 context, if people are on a list but you can't tell  
13 them that they're on a list, you're likely to run into  
14 -- there are likely to be cases where someone is the  
15 victim of a denial of due process, they're wrongly on  
16 the list, but they aren't able to challenge it because  
17 they can't actually even get the information out of  
18 you that they're on the list.

19           We heard earlier today about we've never  
20 learned about -- we've never had any problem with this  
21 thing because we don't know about it. It's sort of  
22 the converse of that. There might be people out there

1 whose due process rights are being violated, but  
2 because you can't tell them you're on this list,  
3 they're not able to try to seek redress for the actual  
4 problem. What do you do? What do you do about that?

5 MR. KENNEDY: Yes, Martha did pass the case  
6 to me. But because it was a state case, it was not  
7 something that -- that particular case was not  
8 something that, obviously, I can comment on because it  
9 was -- that's a state case.

10 But in general, with your point just being  
11 due process, obviously with the new administration and  
12 the focus on transparency, all of the rules and  
13 regulations that are in place obviously will be  
14 reviewed. But from our perspective, even right now,  
15 if you run into a problem is when you actually contact  
16 the DHS program office, and the due process is the  
17 redress process, and it's basically when you run into  
18 a problem.

19 Somebody tells you you can't get on a plane  
20 and you apply to us, one of the things that is pretty  
21 -- that we really kind of look at is if you're not  
22 allowed on a plane, no way, no how, the cat's pretty

1 much out of the bag that something is really kind of  
2 going on. And so we give you additional opportunities  
3 for appeal beyond that which you would get even with just  
4 me. And that's why you have the appeal process to the  
5 assistant secretary of TSA, as well as to the Court of  
6 Appeals.

7           One of the -- the other thing that happens  
8 is if you are on another list, let's say, and you are  
9 repeatedly subjected to additional screening, one of  
10 the things that we don't -- in that case, you're not  
11 denied a privilege. You are actually -- you may be  
12 delayed, but you're not denied the ability to fly.  
13 You're not denied entry into the country.

14           What we do is we try and make sure that we  
15 do not restrict the flow of people and commerce as  
16 much as -- you know, we want to make sure that there's  
17 free and open commerce to the greatest extent  
18 possible. But we will always make sure that the  
19 reviews that need to take place do happen.

20           As for anything else, it really -- like I  
21 said, the redress process is really there for us to be  
22 able to review. And if you do think -- let's say you

1 go through the process and nothing really changes,  
2 there's starting to be a -- there are court cases out  
3 there where people actually do challenge the Federal  
4 government, and not just with what we do but the watch  
5 list in general. So that avenue is definitely open to  
6 an individual.

7 This -- the problem just with watch listing  
8 in general or the -- not the problem, but the issue  
9 with this is we want to be as open as possible, but we  
10 also have to balance that fact that we can't tell  
11 everybody what we're doing. It's one of those that I  
12 didn't make up the rules. It's just the way the rule  
13 is written. But, I mean, that's -- it's one of the  
14 things where we really try to keep people safe, but we  
15 also want to make sure that people can come and go as  
16 they please as much as they can.

17 MR. BEALES: Renard.

18 MR. FRANCOIS: Thank you for coming, and  
19 just to follow on Jim's point, if I am on a watch list  
20 -- excuse me -- and I am not -- I'm denied the ability  
21 to travel, to fly, or delayed, and I go through the  
22 redress program, and you said that you can't confirm

1 or deny that my name is on a watch list, at what point  
2 is it in the appeal process to the assistant secretary  
3 of state maybe, but at what point is it where it is  
4 revisited whether my name is correctly or incorrectly  
5 put on the watch list?

6 MR. KENNEDY: Your -- when you apply for  
7 redress, and let's say that you are a person who is --  
8 your name is on a watch list, what we actually do is  
9 at that time we work with not only the Terrorist  
10 Screening Center but through them with whoever  
11 nominated your name to that list to see if the  
12 information is still valid. So you get a review right  
13 then.

14 The other thing is let's say if you want to  
15 -- let's say you're on the no-fly list and we give you  
16 specific instructions, and you make your -- you avail  
17 yourself of an appeal to the assistant secretary for  
18 TSA, you will get another review at that point. So  
19 you've actually gotten two reviews.

20 But essentially, when you apply to my  
21 office, you actually do get a review at that point.  
22 So we actually look at the information that is

1 contained, and not just my office but also, like I  
2 said, the Terrorist Screening Center and the  
3 nominating agency, to see if it is still appropriate,  
4 and there are cases where we have found that the  
5 information is not correct or it is not appropriate,  
6 and so we will make changes.

7 MR. FRANCOIS: And just a couple of quick  
8 follow-ups to that. In that scenario, is there also  
9 the opportunity for that individual to submit  
10 additional documentation? So there's a problem, I go  
11 through the redress process, and I may think it would  
12 be helpful for you to provide you a copy of my  
13 driver's license and birth certificate to kind of --

14 MR. KENNEDY: It depends on which process  
15 that you have, because it's not just one straight  
16 redress process. It depends on what the issue is.  
17 Let's say that you receive a letter from me that says  
18 no changes are warranted at this time, but if you  
19 would -- this is an interim agency decision, if you  
20 want to have an additional review before the assistant  
21 secretary for final agency decision, you are offered  
22 the opportunity to provide additional data, and there

1 are certain questions that we will ask, and you can  
2 respond to those, as well as additional information.

3 I have received things in my office, I  
4 think the FedEx courier person probably had a backache  
5 when they were done because I had stuff, you know,  
6 pretty high, a lot of documents. So there is --  
7 depending on the redress process, there are cases when  
8 you can actually provide additional documentation,  
9 yes.

10 MR. BEALES: Could I just ask one follow-  
11 up, too? In the transportation cases, the air travel  
12 cases, 1 percent of them are not misidentification.  
13 So they presumably are on a list. How does that break  
14 down of where the determination is you ought to be on  
15 the list versus they get taken off the list?

16 MR. KENNEDY: You mean in the process? Is  
17 that what you're talking about?

18 MR. BEALES: Yeah, in the final  
19 determination. How many of those, of that 1 percent,  
20 how many of them get cleared because -- I mean,  
21 they're not cleared, I guess, but how many of them is  
22 the determination that you are properly on the list as

1       opposed to you're on the list but it's improper and we  
2       change it?

3               MR. KENNEDY: I don't have that statistic  
4       with me. I can get it back to you.

5               MR. BEALES: I would really appreciate  
6       that.

7               MR. KENNEDY: But the number -- we do have  
8       a number of cases, like I said, where we do overturn  
9       the existing -- the person's current status on the  
10      watch list, and we can -- that's something that from a  
11      statistical standpoint, that's something that I can  
12      take back.

13              MR. BEALES: Okay, I would appreciate that.  
14      Thank you very much.

15              David Hoffman.

16              MR. DAVID HOFFMAN: Just a quick question.  
17      I'm wondering if you sort the data by differentiating  
18      how many requests you get from non-U.S. citizens  
19      versus U.S. citizens.

20              MR. KENNEDY: We did not in the past, just  
21      because of the fact that when we opened up the redress  
22      process, we wanted to make sure that it was open for

1 everybody. So initially we did not do that. One of  
2 the things that we are looking at with the new case  
3 management system, as you can kind of imagine, with  
4 all sorts of different ways to slice and dice data,  
5 that is a capability that we will have.

6 Right now we just don't do it, and like I  
7 said, because of the limitations of the system, but  
8 it's something that we will do.

9 MR. BEALES: Ramon.

10 DR. BARQUIN: A little earlier, when we  
11 heard from your colleague on FOIA, I asked about the  
12 convergence with redress, and I want to ask the  
13 reverse. How many of you are -- because it gets back  
14 to this issue of the Catch 22. If I don't know I'm on  
15 the list, how can I ask for redress? But I believe  
16 that a number of these requests to find out if you're  
17 on a list are coming in via FOIA. And how do you work  
18 together with the FOIA side of the house?

19 MR. KENNEDY: Well, what we actually do is  
20 we will -- if somebody sends a FOIA request in, and  
21 what we actually do is we do work with the FOIA office  
22 and say, okay -- for example, there's nothing that I

1 can give you because what you're going to have to do -  
2 - FOIA is not a redress process. So what we actually  
3 did is we told -- there's language that the FOIA  
4 office has that says if you feel that you have been  
5 delayed or denied a right of travel, then please come  
6 to this office, because there's additional information  
7 -- many times what the FOIA office will just receive  
8 is "This happened to me," but we don't have enough  
9 information to really know who you are. There's no  
10 personal information in the initial request. It's a  
11 letter.

12 So what we do is, in order not to do kind  
13 of like the back and forth deal, we say, okay, please  
14 come to this office, either online or sending  
15 something through the mail, or through email, and give  
16 us this information. By the way, and what we actually  
17 do is we actually send them a copy of the information,  
18 the form that we need, as well as the link, so that  
19 the individual can come straight to us so that we can  
20 help to resolve the problem.

21 MR. BEALES: John Sabo.

22 MR. SABO: Just a couple of process

1 questions. When the case is opened, I'm assuming  
2 there's a case number assigned?

3 MR. KENNEDY: Yes.

4 MR. SABO: And does that track to the  
5 individual? In other words, let's say you resolve it  
6 and a month later they fly and they're delayed again  
7 and they come back to you. Do they give you the same  
8 case number and you reopen it, like we do on typically  
9 a lot of tickets? Or do you initiate a new case?

10 MR. KENNEDY: We keep that person's case  
11 number, that individual requester's number. Everybody  
12 that applies for redress gets a redress control  
13 number, and anybody, whether they are misidentified,  
14 whether they are a person whose name is on a watch  
15 list, anybody can -- gets that, gets a case number.

16 And so what we're able to do is if somebody  
17 says, "Well, hey, either, A, I haven't heard anything  
18 from you, or B, I've gone through this process and I  
19 had problems" and they give the redress case number,  
20 well, obviously, we can go into the system and we can  
21 see what happened last time.

22 If they are -- let's say the individual had

1 an issue with just TSA one time, and then now they  
2 flew internationally and they had an issue with CBP,  
3 then we can say, okay, do we have all the information?  
4 Can we reopen this case, yes or no? Or is there some  
5 additional information that we would need from the  
6 individual?

7 So, yes, we are able -- it's just like any  
8 other tracking number. So, yes, we can do that.

9 MR. SABO: Okay. So it really is more of  
10 an identifier. I mean, you could have a much  
11 different circumstance --

12 MR. KENNEDY: Correct.

13 MR. SABO: -- that has nothing to do with  
14 getting on a plane, but you still use the same case  
15 number --

16 MR. KENNEDY: Correct.

17 MR. SABO: -- for the individual. So  
18 you're tracking that. Okay.

19 MR. KENNEDY: The case number is not the,  
20 for lack of a better word -- well, the case number  
21 does not mean -- if you have a case number, it does  
22 not mean that automatically that you're mis-ID'ed or

1 something. It just means that you have applied for  
2 redress.

3 MR. SABO: The other thing is, in your  
4 enhanced system -- I have three questions. But the  
5 second one is for your enhanced system, a lot of the  
6 issues are at the checkpoint, the screening location  
7 for air travel.

8 Does the screening checkpoint, will it have  
9 access to your system? If somebody says, "Well, I've  
10 been delayed, and I understand I've been cleared," and  
11 you go to the back room, is there a way for that  
12 officer to check the case number to see if, in fact,  
13 this person matches? Because they would have an I.D.,  
14 obviously, to get on the plane. I mean, do you have  
15 that type of enhancement in place?

16 MR. KENNEDY: Well, what happens is all the  
17 issues really happen before it gets to the checkpoint.  
18 It really happens when you're at the ticket counter  
19 for the airline. And so right now, when -- the  
20 airlines are all given access to what we call the  
21 cleared list, which are individuals who have applied  
22 for redress before because they have been

1 misidentified, and we give them additional information  
2 on the individual to clearly distinguish that  
3 individual.

4           Now, obviously right now, and I told you  
5 before, one of the things that TSA and DHS is working  
6 on is rolling out Secure Flight, which will actually  
7 take the place of just the airlines doing the  
8 screening and the government actually doing the  
9 screening. So that should actually reduce some of the  
10 misidentifications.

11           As for people at the checkpoint actually  
12 having the access to the system, that's currently not  
13 planned just because of the fact that by the time you  
14 get to the checkpoint, you are already issued a  
15 boarding pass. So the issue is either resolved or you  
16 are going to be screened this way by the time you get  
17 to the checkpoint.

18           So the place that we want to really impact  
19 is really at the ticket counter or the airline's  
20 computer system where you can get your boarding pass  
21 electronically via the Internet. That's where we want  
22 to really impact.

1           MR. SABO: And the last question is in the  
2 appeals process, like to the assistant secretary, is  
3 there a separate appeals staff that independently  
4 examines the complaint and goes back, or do they  
5 simply return the appeal to your staff where you  
6 reevaluate what you'd already done and make  
7 recommendations? In other words, the assistant  
8 secretaries don't work the cases. So is it being  
9 worked by your staff, or is there an independent  
10 appeals staff that looks at it independently?

11           MR. KENNEDY: Well, you have -- remember,  
12 the initial review is done when a person goes up to  
13 the ticket counter and they have an impact. It is  
14 that original -- that review, if you will, is done by  
15 the airline or by their -- within their system as to  
16 if someone is or is not on the watch list, and you  
17 have a process there. You get misidentified, that's  
18 one process.

19           When you come to -- when you apply for  
20 redress and come to my office, then you -- my staff is  
21 the one that makes the review. Now, in the cases that  
22 go up to the assistant secretary, those cases are

1 actually -- everything that we have, and we will do  
2 another check, even on those, and everything that's  
3 done, the assistant secretary and our legal office  
4 will do the -- will review those cases, and it is the  
5 assistant secretary's decision.

6           This is not a huge, huge number. I told  
7 you that I had got -- we've had 51,000 cases, and even  
8 prior to that TSA had its own redress process. But  
9 the number of people that have actually applied for --  
10 that have appealed to the assistant secretary, I think  
11 the number is four. So we kind of get it right.

12           MR. BEALES: As Secure Flight starts to  
13 roll out, will you be able to track whether it is, in  
14 fact, reducing misidentifications?

15           MR. KENNEDY: I don't think I'm qualified  
16 to really answer that question. I think that's more  
17 of a question for the Secure Flight program office.  
18 What we will actually do is continue to offer redress.  
19 If somebody actually comes and says, "Hey, I've had  
20 this problem," we will work the case just like we work  
21 now, but we don't -- I don't -- I'm not the -- I don't  
22 work in the Secure Flight program office, so I don't

1 know what kind of data they will capture on that. So  
2 I think that's probably a get-back for the Secure  
3 Flight program office.

4 MR. BEALES: Is it -- I mean, I guess the  
5 question would be where did the -- do you track where  
6 the misidentification happened, whether it was at the  
7 airline versus at -- you know, in the matching  
8 algorithm that TSA was using? I mean, that's the way  
9 where you would see it, I guess, sort of independent  
10 of what Secure Flight is doing.

11 MR. KENNEDY: We would -- if the person is  
12 mis-ID'ed for us, and we place them on the clear list,  
13 Secure Flight has access to our clear list. So once  
14 you are cleared by redress, then that information goes  
15 over to Secure Flight. And where we would get  
16 involved again and what we want to track again is,  
17 okay, if we cleared the individual and Secure Flight  
18 would -- if there's a problem with Secure Flight after  
19 that point, and then that's when we would actually go  
20 back and work with Secure Flight.

21 But as for up front, that is something that  
22 we can take a look at, but it's not something that we

1 had planned on thus far.

2 MR. BEALES: Okay, because, I mean, it  
3 seems like it would be -- I mean, it seems like it  
4 would be a useful thing to know, and I guess it  
5 depends a little bit on how the rollout of Secure  
6 Flight is actually envisioned. But I assume there  
7 will be a period where there's some matching being  
8 done by Secure Flight and some matching being done by  
9 airlines.

10 MR. KENNEDY: Right, and Secure Flight will  
11 keep those types of numbers.

12 MR. BEALES: Right, right.

13 MR. KENNEDY: Right.

14 MR. BEALES: And knowing whether you're  
15 getting more complaints out of one part of that  
16 process or the other would be a useful thing to know.

17 MR. KENNEDY: We will know our volume. If  
18 it goes up, we will know. Obviously, if it goes up,  
19 if it goes down, those types of things, yes. And the  
20 beauty of any type of COTS case management system is  
21 for the type of information that we collect that can  
22 be sliced and diced a number of different ways. So if

1 that's something that we need to take a look at in the  
2 future, we will have the ability to do that, yes.

3 MR. BEALES: Okay. Are there other  
4 questions from the committee?

5 [No response.]

6 MR. BEALES: All right. If not, then thank  
7 you very much for being with us. It's been very  
8 helpful.

9 We will move now to subcommittee reports,  
10 and then that will be followed by public comment. So  
11 if you are interested in making a public comment,  
12 you're approaching the last chance to sign up on the  
13 table outside. And then we will turn to public  
14 comments when we're done with the subcommittee  
15 reports.

16 The Subcommittee on Data Acquisition and  
17 Use, Richard and David.

18

19

20

21

22



1 calling the sharing threshold analysis, and that would  
2 be an examination of the request and asking the  
3 requester to provide enough information to make  
4 certain that the request is going to comply with the  
5 Department's fair information principles, that it is  
6 adopted for how it will handle personal data, and that  
7 you can have confidence that the entity that will be  
8 receiving the data has the right mechanisms and  
9 staffing in place to be able to protect the data.

10           The second part of the life cycle, then,  
11 would be a template sharing agreement, and that  
12 template sharing agreement would need to have  
13 components within it to provide for robust privacy and  
14 information security protection for the information.

15           The third part of that would be  
16 communication within the affected component to make  
17 sure that it understands how to manage that agreement.

18           The fourth would be monitor -- a process  
19 for monitoring compliance with agreements once they  
20 are entered into.

21           And the last would be a process for  
22 auditing how that entire process is doing in feeding

1 back recommendations into management.

2 So with that life cycle process in place,  
3 we are thinking that what needs to be on top of that  
4 is certain governance and operations mechanisms to  
5 make sure that it runs effectively.

6 The first that we are preliminarily  
7 exploring at this point as a recommendation is the  
8 creation of an information sharing agreement review  
9 board for the Department that would be able to provide  
10 oversight and governance.

11 The second would be a secretary mandate for  
12 the components that would need to implement this, and  
13 it would need to be implemented by component chief  
14 privacy officers.

15 The third would be a training component for  
16 the individual component CPOs and for those that are  
17 proposing doing the sharing.

18 And the fourth would be a communication of  
19 process and -- of the process and requirements  
20 throughout the Department and other U.S. Government  
21 agencies, and other state, local, or foreign agencies  
22 with whom the sharing will potentially occur.

1           So once again, those are all preliminary  
2       recommendations that we are working out at this point,  
3       but we wanted to provide a robust and detailed update  
4       for everyone so that everyone would know the major  
5       concepts that we're working with.

6           MR. BEALES: That's useful.

7           Are there comments or questions?

8           [No response.]

9           MR. BEALES: All right. The Subcommittee  
10       on Data Integrity and Information Protection, Ramon.

11          DR. BARQUIN: We have been in conversations  
12       with the Privacy Office in relation to a tasking  
13       related to the need for privacy compliance with  
14       service-oriented architecture, which is the DHS stated  
15       direction.

16          We have been somewhat handicapped by the  
17       lack of sufficient members, active members in this  
18       subcommittee. But nonetheless, we have at least  
19       developed what we think is a six-point plan.

20          The first step, which is very, very  
21       important, has to identify the drivers that are really  
22       pushing for this. In other words, where's the pain

1 that requires privacy compliance at the SOA level?

2 The second is we've asked the Privacy  
3 Office to at least do some of the due diligence vis-à-  
4 vis research and review of what has been done, if  
5 anything, either in other agencies that are  
6 implementing or have implemented SOA in the Federal  
7 government or in the private sector.

8 And with those two steps positively  
9 accomplished, out of the way, then we would move to  
10 actually then be briefed by the Privacy Office on  
11 their objectives and approach; next, review the  
12 relevant documentation and materials that are  
13 currently being used as case examples, and we have  
14 seen at least one that was dealing with the PCQS  
15 system in a SOA environment at USCIS. PCQS is Person  
16 Centric Query System at USCIS.

17 Then we would want to meet with the  
18 appropriate stakeholders not just in the Privacy  
19 Office but within the office of the CIO that are  
20 actually in charge of implementing the SOA.

21 And then as our last step, we would develop  
22 some draft -- some draft guidelines to present to the

1 full committee, then, for approval. So that's where  
2 we are.

3 MR. BEALES: All right. Questions?  
4 Comments?

5 [No response.]

6 MR. BEALES: All right, then. Let's turn  
7 to the Subcommittee on Privacy Architecture. Jim?

8 MR. HARPER: We have one pipeline project  
9 that, unfortunately, seems to be in a very long  
10 pipeline, but we're looking forward to progress on  
11 that in the near future, which is the question of DHS  
12 grants to states. Funds are going out now to states  
13 for programs that may have privacy consequences, but  
14 we don't have any information on that. And so the  
15 starting point we were seeking was to even get  
16 information about whether they were privacy  
17 consequential programs.

18 Joan has been exceedingly patient with  
19 staff and with the prior privacy officer, from whom we  
20 believe we had a commitment to get that into the  
21 process last year, but it didn't happen. So we're  
22 very eager and expect great work from the staff to

1 help us with this program going forward, and expect  
2 that by fall we'll at least have something in the  
3 grant-making process that at least reveals the  
4 possibility of privacy consequential grants from DHS.

5 We spent time yesterday essentially  
6 brainstorming about the things that we would like that  
7 we think might be helpful to the new privacy officer  
8 going forward. Also, because it was mentioned in the  
9 letter that we recently sent to the secretary. We  
10 think that enhanced driver's licenses are an important  
11 area that would be worthy of study.

12 It's interesting because that may be  
13 shaping up as the alternative to Real ID. For all its  
14 faults, Real ID at least was a legislatively created  
15 program that went through the regulatory process,  
16 Notice of Proposed Rulemaking and so on and so forth,  
17 where EDLs are going forward outside of a regulatory  
18 process. And so it's something that should probably  
19 get some examination.

20 Another that really took wing today, this  
21 morning, was the question of ISO standard-making  
22 processes in the privacy area. I think the Privacy

1 Architecture Subcommittee is probably well suited for  
2 that, especially because John Sabo is extremely  
3 knowledgeable and participating in some degree with  
4 the groups that are working on this. So this is  
5 something that our subcommittee is very interested in  
6 working on.

7 Other cool ideas have been floating around,  
8 but these are the top level.

9 MS. McNABB: And if I can just add one  
10 thing. In case you're going to ask, or in case Martha  
11 is going to ask about agenda items for the next  
12 meeting, we'd like to have an update on EDL and Real  
13 ID from the Office.

14 MR. BEALES: Okay. That makes a lot of  
15 sense.

16 All right. In that event, it is now time  
17 for public comments. We have at least one request for  
18 public comments, and Martha, I see, is checking to see  
19 if there are any others. But we will begin with  
20 Jeremy Epstein from SRI International.

21

22

1 PUBLIC COMMENTS

2 MR. EPSTEIN: Good afternoon. [Inaudible.]

3 With regard to this morning's discussion of the FOIA  
4 issues, I had a couple of thoughts that I wanted to  
5 share and ask your opinions on. The first was --

6 COURT REPORTER: I apologize. Would you  
7 come use -- this mic isn't plugged into our recording  
8 system. I apologize. Right here would be great.

9 MR. EPSTEIN: Do you want me to start over  
10 for recording purposes?

11 COURT REPORTER: Sure.

12 MR. EPSTEIN: So with regard to this  
13 morning's discussion of FOIA, I was wondering whether  
14 -- well, I first wanted to comment that the -- I  
15 apologize. The method that's used through the credit  
16 bureaus for verifying identity is not all, in my  
17 opinion, that it's cracked up to be.

18 As an example, when I went to get my credit  
19 report, they asked me questions like who holds your  
20 mortgage? Well, in many places that's a matter of  
21 public record. Additionally, there are a few big  
22 mortgage holders that hold nearly all of the mortgages

1 in the United States. So if you're given a choice  
2 between Third Bank of Oshkosh and Countrywide  
3 Financial, the odds are pretty good you can guess the  
4 answer.

5 Similarly, they asked me who held my credit  
6 card, and if the choice is the Bank of Midland, Texas  
7 or Chase Bank, you have a pretty good chance of  
8 getting the right answer just by guessing.

9 So my point is that these sorts of  
10 questions that are used are a great idea in principle  
11 based on the idea that they have more information than  
12 you have or -- excuse me -- they have more information  
13 than is public, but it may not be as good as you think  
14 it's going to be in actually authenticating a person.

15 And on the flip side, I wanted to ask about  
16 the impact of social networks like Facebook in the  
17 FOIA process. For example, if I've chosen to make  
18 public a lot of information about myself, maybe a FOIA  
19 request by somebody else about me should release more  
20 information than it otherwise might because I've  
21 already made the information public. And conversely,  
22 if I've released information about myself on Facebook

1 or something like that, then it may be harder to  
2 verify my identity because there's so much information  
3 about me publicly.

4 So I guess I'd sort of throw those out and  
5 see if there are any opinions about how any of these  
6 social networks and/or credit bureau issues affect any  
7 of these privacy issues we were discussing this  
8 morning with FOIA.

9 MR. BEALES: John?

10 MR. EPSTEIN: I know that was open-ended.

11 MR. SABO: No, no. On your last -- on the  
12 social networking, could you sort of clarify a little  
13 bit in the sense -- are you -- I mean, an agency may  
14 have a request for disclosure. Let's say it's Privacy  
15 Act data and it's not just FOIA, like what do you have  
16 on me, but even in that case, but Privacy Act data.  
17 Are you suggesting that because information may be on  
18 Facebook, there should be some linkage to the  
19 authentication system used by DHS, and the more data  
20 that's on an external public source, then there has to  
21 be a linkage because that implies a system linkage to  
22 Facebook?

1           MR. EPSTEIN: I'm suggesting that it cuts  
2 both ways, that because there is -- and I used  
3 Facebook as an example. It's obviously no different  
4 for any other social network. I was reading a  
5 friend's Facebook the other day where she had -- there  
6 was one of these quiz things, 25 facts about yourself  
7 sort of thing, and it asks you to put together your  
8 father's first name, your grandfather's first name,  
9 and your great-grandfather's first name, et cetera.

10           That's the sort of information that might  
11 be used as an authenticator in some cases, but here it  
12 is in her case, she put it on Facebook. I didn't put  
13 information like that on my Facebook page. So that  
14 might reduce the ability, because of the existence of  
15 it on Facebook, it may reduce the ability as an  
16 authenticator.

17           MR. SABO: Okay, so I get it now. So your  
18 point might be a research question. In other words,  
19 the common availability of that type of personal  
20 information, voluntarily given by citizens or  
21 whatever, would impact your authentication methodology  
22 used by government. And that could potentially be a

1 research question to some degree.

2 MR. EPSTEIN: Right, and the converse as  
3 well. For example, a lot of college kids these days  
4 put all sorts of information about clubs they're  
5 interested in. If the question as part of a FOIA  
6 request comes up, well, should you be -- should they  
7 release information about what clubs they know you're  
8 a member of, maybe they don't need to safeguard that  
9 information, while previously they might have. In my  
10 generation, they might have not disclosed that  
11 information because that would be considered private  
12 information, and now it's not private anymore.

13 MR. BEALES: Jim Harper.

14 MR. HARPER: I think your -- I just want to  
15 say, your point is well taken. The problems you raise  
16 are inherent to the idea of epistometric identifiers.  
17 It does have to be -- it has to be knowledge that both  
18 have and has to be knowledge that others generally  
19 don't have. And so you'll have to strike careful  
20 balances.

21 But if it's about travel information, the  
22 TSA may have the information on the person. What's

1     your favorite airline?  What's the airline you  
2     traveled on most recently?  Those kinds of questions  
3     narrowly drawn can get you pretty darn close, and I  
4     think one of the most important questions or moving  
5     parts in that machinery is the amount of security you  
6     need for the particular inquiry.

7                 I think for the majority of the public, the  
8     stuff that they're going to get back from a FOIA  
9     request is actually not that significant, and so you  
10    don't need to have really, really tightly wound down  
11    identification procedures in order to be able to  
12    release it.  If you get it wrong, it's unfortunate,  
13    but you're not going to cause real damage to some  
14    party.

15                MR. EPSTEIN:  And the balance is going to  
16    change over time as people put more and more  
17    information out in the public domain.

18                MR. HARPER:  Absolutely, yes.

19                MR. EPSTEIN:  Thank you.

20                MR. BEALES:  David?

21                Joan.

22                MS. McNABB:  Now, I was getting confused

1       there, Jim. With a FOIA request, you don't need to --  
2       you can be anybody, right? I don't need to  
3       authenticate myself for a straight FOIA request,  
4       right? It's a first-party request or a Privacy Act  
5       request where there's an issue of authentication.

6               MR. EPSTEIN: I'm sorry. Yes. I should  
7       have said for a Privacy Act request. But the other  
8       part of it would relate to --

9               MS. McNABB: It was Jim. It was Jim I was  
10      talking to. You said it right.

11              MR. HARPER: I said it wrong.

12              MS. McNABB: Yeah.

13              MR. HARPER: Thank you, Joan.

14              MR. BEALES: Isn't it the same question,  
15      though? Because what you can get under the FOIA if it  
16      is privacy sensitive information depends on who you  
17      are. I mean, if it was your FOIA about you, there  
18      wouldn't be an issue of telling you what you knew if  
19      it was really you. I understand there's the same  
20      issue with Privacy Act access, but isn't there under  
21      FOIA too?

22              MS. McNABB: Well, the way it works in

1 California State government, which is modeled on the  
2 Federal process, is if I make a request and I say it's  
3 a Public Records Act, a FOIA request, but it's about  
4 me, it's treated as if it's a Privacy Act request. If  
5 it's not -- if I don't -- if it's not about me, if I  
6 don't say it's about me, it's a Public Records Act  
7 request.

8 MR. EPSTEIN: Maybe I could give a  
9 specific. I apologize for taking so much time on  
10 this. But if someone filed a FOIA request that  
11 involved what countries I've traveled to, that might  
12 be something that ordinarily would be private  
13 information.

14 However, if you go to look at my Facebook  
15 page, my Facebook page actually does list all the  
16 countries I've been to. And so maybe they wouldn't  
17 need to protect that information, while in an earlier  
18 generation they would have.

19 MS. McNABB: Yeah, and that's sort of a  
20 legal issue about what our definition of privacy is.  
21 Once something has been made public to a third party,  
22 is it private anymore?

1           MR. BEALES: Well, but there's a practical  
2 issue too, because in a world where some people put  
3 that on their Facebook page and other people don't,  
4 unless we want DHS to check everybody's Facebook --

5           MS. McNABB: We don't. We don't.

6           MR. BEALES: Which we probably don't,  
7 there's no practical way to distinguish.

8           John. We may be able to get some facts  
9 here.

10          MR. KROPF: A point of some information for  
11 the group. I think that what we're talking about here  
12 is a concept that's known in FOIA as waiver. And if  
13 the government officially has information in its  
14 records and officially releases that information, it  
15 has waived its right to protect it against all other  
16 requesters. However, if an individual on their own  
17 goes to their own Facebook page and decides to post  
18 whatever it is that they want to about themselves,  
19 that information perhaps might match up or not with an  
20 official government record, that does not waive any  
21 protection that the government might assert in  
22 response to a FOIA request.

1                   So, one, the Facebook would not waive the  
2 rights of the government to protect it in the FOIA  
3 realm, if that helps.

4                   MR. BEALES: Thank you.

5                   Lance.

6                   MR. LANCE HOFFMAN: Again, this is -- we  
7 start getting into animated discussion on these  
8 things, and this is the kind of thing, I'll say it  
9 again, since I foreshadowed it, but Jim didn't pick up  
10 on it, I think the Privacy Office could somehow  
11 sponsor or get to happen workshops on suitable topics  
12 like this which are going to come up more. In  
13 particular, the thing that came up here.

14                   Third-party provision information access  
15 and, oh, by the way, these third-party applications,  
16 how do you trust them anyway, all these sorts of  
17 things. We don't want to be -- we want to be in front  
18 of the curve, not behind the curve on them. I think  
19 it may be worth looking at or recommending to the  
20 secretary and the CPO that we look at it after we have  
21 suitable discussion on it.

22                   MR. BEALES: All right. Any other

1 questions? Reed.

2 MR. FREEMAN: There was mention earlier  
3 about things we'd like to see. I think Joan mentioned  
4 some things that she'd like for the next meeting. And  
5 in that vein, I'd like to ask my colleagues around  
6 this table if they'd agree that more information on  
7 this ISO process would be a nice addition to the next  
8 meeting.

9 And the things that come to my mind on  
10 this, having heard of it for the first time today, are  
11 what, by then, what will have been the Department's  
12 involvement in it, and what positions will they have  
13 taken. Who are the other participants in this? I  
14 know from the private sector, none of my clients have  
15 been asked to participate.

16 What is the status of the process? What's  
17 the timeline and next steps? And are there any public  
18 documents about this? And if so, can we have them?  
19 Do we have unanimous consent on that?

20 MR. BEALES: We have already started the  
21 process of inquiring about some of those things. I  
22 mean, I think that's a good list, Reed, and I think it

1 probably is something that ought to be on the agenda  
2 for our next session, and probably on a subcommittee  
3 agenda as well. I thought this was a scary discussion  
4 this morning, and we certainly ought to pursue what's  
5 going on and try to see if we can't be helpful about  
6 managing that process.

7 MR. FREEMAN: Thank you.

8 MR. BEALES: Other questions or comments?

9 [No response.]

10 MR. BEALES: If not, then I guess we have  
11 reached the time to adjourn the meeting. Thank you  
12 all for being here. It was good to see you all again,  
13 and we will meet again in September. In May. Skipped  
14 a month.

15 [Whereupon, at 2:55 p.m., the meeting was  
16 adjourned.]

17

18

19

20

21

22