

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

Wednesday, December 3, 2008

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

2 MR. HUNT: Good morning, and welcome to the
3 public meeting of the Department of Homeland Security
4 Privacy Office's Data Privacy and Integrity Committee
5 meeting.

6 My name is Ken Hunt. Under the Federal
7 Advisory Committee Act which governs the operations of
8 advisory committees, a Designated Federal Official is
9 -- must be present for all public meetings. I am the
10 Designated Federal Official for this committee. And
11 so, having passed that threshold requirement, I will
12 turn the meeting over to the -- to the Committee Chair,
13 Lisa Sotto.

14 MS. SOTTO: Thank you. Actually, Vice Chair.
15 Howard Beales, who is our Chair, was not able to join
16 us today, and sends his regrets.

17 So, welcome, to my fellow committee members,
18 I am delighted to see all of you here. And welcome, to
19 our public participants, as well.

20 This is our last meeting for 2008, and we are
21 looking forward to wrapping up ongoing projects, and
22 also looking forward to taking on some new projects in

1 2009 and assisting with the transition in any way that
2 we can.

3 A couple of quick introductory items. If you
4 could turn off your cell phones, please, we would very
5 much appreciate that.

6 And if you are interested in signing up for
7 the public comment period, the list of folks who are
8 signing up is outside the room. So, please do sign up;
9 we would love to hear from you.

10 With that introduction, I'd like to turn the
11 mike over to Huge Teufel to tell us what's been going
12 on at -- in the Privacy Office.

13 Just a quick introduction of Hugo -- if I can
14 find the right sheet -- sorry, Hugo. I'm looking.
15 Well, Hugo, I'm going to let you introduce yourself,
16 because I can't find the right sheet, here.

17 [Laughter.]

18 MR. TEUFEL: Okay.

19 MS. SOTTO: Sorry 'bout that.

20

21

22

1 DHS PRIVACY OFFICE UPDATE

2 MR. TEUFEL: Good morning. I'm Hugo Teufel.
3 I'm the Chief Privacy Officer at the Department of
4 Homeland Security. And this, as Lisa mentioned, is the
5 last meeting of the Advisory Committee for 2008, the
6 last meeting before the change of administration, and a
7 very exciting time in Washington and at the Department
8 as we see changes in policies and personnel and other
9 things.

10 I have been -- well, let me back up. I had
11 thought about what I wanted to talk to you all today,
12 and rather than just focusing on the things that we've
13 done over the last few months, I wanted to -- I wanted
14 to quickly go over the things that we've done in the
15 office in the two and a half -- almost two and a half years
16 that I have had the honor and privilege of serving as
17 the Privacy Officer.

18 And let me just say, over the last month or
19 so has been an exciting time for me, in the way that
20 the Chinese talk about, "May you live in exciting
21 times." My wife gave birth to our second daughter, and
22 so, we're not sleeping. And our older daughter managed

1 to give me a bug that managed to stay with me, in one
2 form or another, for all of November, and so, this is
3 the first week that I'm back and functioning. The --
4 some of the last vestiges of the bronchitis that
5 developed as a result of that bug are still with me,
6 and so, I'd ask your indulgence if I have to cough from
7 time to time. But, it's almost gone. And Tom knows,
8 because Tom and I have met, on a couple of occasions,
9 on some issues, over November, and sometimes it was --
10 it was difficult just to get down to Tom's office, let
11 alone talk about substantive issues. But, I am here
12 and almost healthy, and glad to be here.

13 So, I came into the office in 2006, July of
14 2006, having served as Associate General Counsel for
15 General Law at the Department for two and a half years,
16 and having been the lawyer who oversaw, among other
17 things, the provision of legal advice to both the
18 Privacy Office and the Office for Civil Rights and
19 Civil Liberties.

20 I started at the Department in January of
21 2004, which brought me within a week of the one-year
22 anniversary of the effective date of the Homeland

1 Security Act, but put me at about the 10-month -- 10-
2 and-a-half-month mark for the first year, leading up to
3 the opening of the Department, in March of 2003.

4 Again, I started in January of 2001.

5 And looking back at that period -- of course,
6 I wasn't here in 2003, but a lot of my colleagues and
7 friends who I knew from previous lives were here in
8 2003 -- being here at the Department, 2003-2004, just
9 getting an office up and running was a substantial
10 success at the Department. The difficulty with which
11 folks at the department level were able to get things
12 done cannot be overestimated or overemphasized today.
13 It was very, very difficult. And so, I say this
14 because when I came into the office, in 2006, I was --
15 I was terribly impressed by the folks that my
16 predecessor had hired. Without question, the Privacy
17 Office team is the absolute best team in the public
18 sector for privacy and privacy policy.

19 And the other thing that I want to mention,
20 that my predecessor did a -- just, an outstanding job
21 of, was thinking about the structure of the office and
22 the things that the office needed to focus on. I've

1 been in government -- at this point, today, I've been
2 in government for about 11 or 12 years, not including
3 -- not including military service, and not including
4 service at the state level, and I've worked at a number
5 of departments. And the work that Nuala did, in
6 setting up the office and thinking about the things
7 that we needed to focus on, was outstanding. And the
8 key thing here comes right out of the organic statute
9 for the Homeland -- for the Privacy Office, Section 222
10 of the Homeland Security Act, and that is that our
11 office is the primary office for privacy policy.

12 If you think about privacy in government from
13 1974 up until today, too often privacy professionals
14 within Federal agencies were not advisors and
15 counselors on privacy, they were technicians, they were
16 people who made sure that the boxes were checked, that
17 there were Systems of Records Notices in place; and
18 after the e-Government Act, that there were privacy
19 impact assessments in place. But, really it was about
20 checking the box and doing what was required by law,
21 not thinking about policy, not thinking about what we
22 ought to be doing, but, rather, what does the law

1 require us to do, and that's what we're going to do,
2 and often nothing more.

3 Having said that, when I came into the
4 office, I had some concerns. We'd only gotten out one
5 annual report, and folks up on the Hill and in the
6 privacy advocacy community were, rightly, very unhappy
7 about the fact that in -- at that time, which would
8 have been a little over three years since the Department
9 had been stood up, we'd gotten out one annual report.
10 There were a couple of other reports that were
11 outstanding, that were some months overdue.

12 Also, we had about 12 to 16 Federal
13 employees, including -- not including me, as the Chief
14 FOIA Officer, but including one sole Federal employee
15 handling FOIA matters at the Department level. We had
16 a backlog of over 100,000 FOIA requests and FOIA
17 appeals. And we had over 200 legacy agency Systems of
18 Records Notices that we had not gotten to. Moreover,
19 in the three-plus years that we had been in existence, we
20 had not ever received a budget increase.

21 So, I sat down with the folks in the office,
22 and I said, "What is it that we're doing that we're

1 required to do? What is that we're doing that we're
2 not required to do that we ought to be doing? What is
3 it that we're not required -- that we're required to
4 do, but we're not doing? What are the things that we
5 need to focus in on? What do we need to get done
6 during the time that I'm in the office?"

7 And so, we looked at how we could better
8 integrate ourselves into the Department, how we could
9 get work out in a more efficient manner, and how we
10 could do a better job of protecting privacy, and,
11 really, baking privacy in at the outset.

12 So, we worked very hard to increase our
13 involvement in -- at the earliest stages, our
14 involvement in new programs. I was able to draw upon
15 my relationships that I had established in the two and a
16 half years previously in the General Counsel's Office.
17 We were able to, for the first time, get a budget
18 increase of over a million dollars. In the two and a
19 half years that I've been in the office, we went from
20 12 to 16 full-time employees to about 30 full-time
21 employees, with a few slots that we still have to hire.
22 The FOIA side of the house went from one lone FOIA

1 employee, who now is our Deputy Chief FOIA Officer, to
2 over five.

3 We have issued privacy policy guidance,
4 something we had not done before, to include our
5 memorandum on mixed-use systems, administratively
6 extending the Privacy Act to non-U.S. citizens, non-
7 LPRs, and we are, to my knowledge, the only Federal
8 agency that has done that. We've issued a number of
9 guidance documentation within the Department, to
10 include our privacy incident handling guidance. We
11 recommended to the Secretary that component privacy
12 officers be added in components where personally
13 identifiable information was a critical aspect of that
14 component's mission. And the Secretary agreed, and
15 four out of the six components have hired component
16 privacy officers, and we hold out hope for the other
17 two components.

18 Since I came into office, we've gotten out
19 three annual reports, and each has been better than the
20 last.

21 On the FOIA side of the house, in large part
22 because of the efforts of our FOIA team, we have seen a

1 30-percent reduction in the number of FOIA -- in the
2 FOIA backlog, 30 percent. And remember, we were up at
3 over 100,000 when I came into the position.

4 Something that we're wrapping up this month
5 is the legacy SORN project. About a year ago, after
6 realizing that we'd made absolutely no progress in
7 getting the legacy agency SORNs reviewed and revised,
8 consolidated, or retired, as necessary, I sat down with
9 our Director of Compliance and our Deputy Chief Privacy
10 Officer and said, "We've got to do something about
11 this. And if we can't do it in-house, when we've got
12 to bring in contractors to get that done." I am very
13 pleased to tell you that the vast majority of the
14 components have had their legacy SORNs reviewed,
15 revised, consolidated, and/or reissued as DHS SORNs.
16 The -- there are a few components, who I don't want to
17 mention here -- we will be wrapping up those SORNs at
18 the end of the week. And with the exception of maybe a
19 couple of last-minute SORNs for the Department's Office
20 of Security, we anticipate that this Friday we will
21 have all of the legacy agency SORNs reviewed, revised,
22 consolidated, retired, or reissued. All of that work

1 will have been done and will be published in the
2 Federal Register, and the 30-day periods will have run
3 on the NPRNs for exemptions, before January 20th.

4 We've also run a number of workshops, to
5 include workshops on data mining and CCTV. And I
6 anticipate that we will get out our documentation on
7 CCTV best practices and our data-mining report sometime
8 before the end of 2008, because I don't plan on leaving
9 anything on my plate when I had that over to the next
10 administration. We will have everything done before I
11 go out the door.

12 One final thing I want to talk about is the
13 international side, because it was something that I
14 didn't have a lot of experience in, but I learned
15 quickly.

16 This morning, I received an e-mail from the
17 U.K. Cabinet Office. Two of our staff from the
18 international privacy policy side and our Director of
19 Compliance were over in the United Kingdom last week as
20 part of an ongoing series of exchanges that our office
21 is engaged in with various data-protection authorities
22 in Europe. And our two -- our two Privacy Office folks

1 were over in the U.K. Information Commissioner's Office
2 last week, and also had meetings with the U.K. Ministry
3 of Justice and the U.K. Border Agency. And at one of
4 those meetings were some folks from the U.K. Cabinet
5 Office that I had some dealings with through our -- the
6 office's good friend Peter Cullen. And we gained a
7 great deal better appreciation, as did they on our
8 system -- but, we have a much better appreciation of
9 the U.K. approach to data protection as a result of
10 that.

11 This project started out, some months back,
12 when we approached the Canadian Privacy Commissioner
13 and suggested that it would be helpful to both sides if
14 we engaged in exchanges to better understand public-
15 sector approaches in the two countries. Jennifer
16 Stoddard agreed and sent two of her staff down to work
17 with us. We followed up with someone from the Spanish
18 Data Protection Authority's Office coming out and
19 spending a week with us in September. And I anticipate
20 that, sometime in the next couple of months, Alex Turk
21 will send a couple of his staff from the CANEAL over to
22 spend time in our offices, as will, later on next year,

1 our colleagues from the German Data Protection
2 Commissioners Office.

3 But, one of the things that we gathered as I
4 got more involved in international data-protection
5 issues and as we worked on things such as the high-
6 level contact group and discussions with the Europeans
7 over the passenger name record data, is that, frankly,
8 in the United States, at least at the Department of
9 Homeland Security, we do a pretty good job of
10 transparency -- in fact, we do a really good job of
11 transparency -- but, one thing that was -- became clear
12 to me is that we, in the United States, did not have a
13 good understanding of at least one aspect of the
14 European approach to data protection, and that is that
15 it was -- it is not clear to any of us -- and if it's
16 clear to any of you, I would be very surprised, because
17 we've read a lot of the literature and we've talked to
18 a lot of folks within the United States -- that there
19 is -- there is very little understanding about how data
20 protection works in the context of law enforcement,
21 intelligence, and security agencies. And so, over a
22 year ago -- in fact, about a year and a half ago --

1 Jane Horvath and I, when she was the Privacy and Civil
2 Liberties Officer at the Department of Justice, after a
3 high-level contact group meeting in Brussels, decided
4 that we would write some letters so that we could
5 better understand the uniquely European -- and I
6 shouldn't say "uniquely," because there are other parts
7 of the world that do this -- the European approach to
8 the commercial collection of personally identifiable
9 information for security agency use -- and, in
10 particular, I'm referring to hotel registration,
11 personal data, something that's not done in the United
12 States, but in the Middle East and in Europe, is quite
13 common, that whenever a guest checks in to a hotel,
14 hostel, a campsite, anyplace where people have
15 temporary lodging, the innkeeper collects certain
16 personally identifiable information that either is made
17 available to the law enforcement or security
18 authorities or, in some cases, is transmitted every
19 night electronically to the security services.

20 We've learned a great deal. And we have
21 been, frankly, surprised at some of the things that we
22 have seen. And I anticipate, within the next month or

1 so, we will be issuing a public report, an interim
2 report, talking about the things that we have found.
3 And I don't want to go beyond that, but I do want to
4 tell you about it, because far too often in the United
5 States there are those here who advocate that we should
6 take the European approach to data protection, but I
7 submit to you that there is not a full understanding in
8 the United States of how data protection works, and,
9 most importantly, in the area of intelligence, law
10 enforcement, and security services. And there is --
11 without question, there will be increasing
12 transatlantic data-sharing efforts between the United
13 States and the Europeans, and it is critical that we
14 understand, better, how their systems work if we are
15 going to engage in further data sharing.

16 So, with that, I will stop, and I believe we
17 have Catherine Papoi, who is our Deputy Chief FOIA
18 Officer, and who also has been serving as part of the
19 transition team, and I think she's going to talk to you
20 about transition efforts.

21 Unfortunately, because my time is short --
22 and not just here, but in the office -- I will be

1 coming and going from today's meeting, because there
2 are a number of things that I have yet to get done, to
3 include probably encouraging folks at components to
4 wrap up work on the legacy SORN project so that we can
5 meet that December 5th deadline.

6 So, with that, I will stop. And I've got,
7 maybe, a couple of minutes for questions, if you have
8 any.

9 MS. SOTTO: Thank you so much, Hugo. And my
10 apologies for not having your bio at the top of my list
11 here.

12 If anybody has questions, please raise your
13 name tents.

14 Okay. David, please.

15 MR. DAVID HOFFMAN: Hugo, more of a comment
16 that I was thinking maybe you could expand on. One of
17 the things that I thought was notable in the most
18 recent report that you sent out was the incredible
19 progress in creating privacy officers in the individual
20 Department components. And that seems to be a huge
21 accomplishment that has come together over the past
22 year. And I was wondering if you could talk just a

1 little about where you see that at now and what you
2 expect that that will look like in, maybe, the next 12
3 to 18 months.

4 MR. TEUFEL: I suspect that there will
5 probably be more component privacy officers. I think
6 there'll be -- I think there'll be a lot of changes
7 around the Executive Branch with respect to privacy
8 officers, but I think, at the Department, there will --
9 there will likely be some additional component privacy
10 officers. I know that there is some legislation that's
11 been working its way through Congress that would
12 mandate component privacy officers at some -- not just
13 the components that we've listed, but a few others.

14 The biggest resistance that I've seen to
15 component privacy officers really is this -- is this
16 technician's approach and the mentality that, "All that
17 is needed are technicians in some of the components,"
18 that are -- that came from legacy agencies and did
19 things the way those legacy agencies did things. But,
20 what you have to appreciate, and I know that this
21 committee does, is that the -- that the one thing that
22 binds this Department together, the thread that ties

1 together all of the various components at the
2 Department, is information -- in particular, personally
3 identifiable information. And for this Department to
4 have the trust and confidence of the American public
5 and the traveling public, it has to have more
6 transparency, it has to show what it's doing with the
7 public's information. I think we've done a pretty good
8 job. I don't think we've been able to get that message
9 out to the public as well as we would like, but I can
10 tell you, from having worked on the inside, that we've
11 really done a great job and we've really made great
12 improvements, in terms of protecting privacy at the
13 Department. So, I anticipate that there will be more
14 component privacy officers. We'll have to see what the
15 next administration wants to do. I have some thoughts,
16 and I'd be happy to share it with whoever my successor
17 is. But, beyond that, can't think of what else to say
18 to -- in answer to your question.

19 MR. DAVID HOFFMAN: Thanks.

20 MS. SOTTO: Ramon, please.

21 DR. BARQUIN: Hugo, we've heard about
22 accomplishments, and I think you've done a heck of a

1 lot, but as you walk out the door, what, in your mind,
2 are the top two truly, truly important things that you
3 feel you have not accomplished that you will pass on to
4 the --

5 MR. TEUFEL: I don't know if I can --

6 DR. BARQUIN: -- next administration?

7 MR. TEUFEL: -- limit it to two. I'm not sure
8 I could limit it to two. There's a lot of stuff that I
9 would have liked to have done. I think the biggest
10 thing -- it's not so much what I didn't, but, for me,
11 the thing that I get -- derive the most satisfaction
12 from is getting out of the way, clearing the decks of
13 all of the stuff that needed to be done so that the
14 next person, when he or she comes in, doesn't have to
15 worry about, "Okay, do you have policies in place that
16 address these issues? Okay, have you -- have you
17 looked at all of the old Energy Department, Justice
18 Department, Transportation and Treasury Department
19 Systems of Records Notices, that really were all over
20 the board, in terms of how they were done? Have you
21 cleared that stuff up?" And the importance of getting
22 all of that stuff done is that my successor, when he or

1 she comes in, will be able to focus a lot more than I
2 was on the real mission of the Department, and that is
3 the provision of privacy policy advice and guidance to
4 the Department. I'm not saying that we didn't do that.
5 We did. But, what I'm saying is that there were things
6 that needed to be taken care of, and it would be -- I
7 would have failed in my mission if I did not get those
8 things taken care before I went out the door.

9 So, in terms of -- so, having answered that
10 -- and that really is the big one, as far as I'm
11 concerned -- going beyond that, there's an -- we didn't
12 get the FOIA and Privacy Act regulations out. We
13 worked very, very hard for the better part of the two and
14 a half years that I was in the office, and we didn't
15 get those done. But, we'll have them teed up for the
16 next administration.

17 We still have some significant backlogs in
18 FOIA, and we did a lot of -- we did a lot of good work,
19 but there's a lot that needs to be done.

20 I -- in fact, I would say that, generally
21 speaking, the area of freedom of information, there's a
22 lot more work to be done, and I know Catherine -- when

1 my successor comes in, Catherine Papoi, our Deputy
2 Chief FOIA Officer, is going to be very, very, very
3 busy in getting the things done that need to be done.
4 We probably need to be staffed up in the FOIA area, not
5 just at the Department, but in the components, as well.

6 Data Integrity Board and Computer Matching
7 Agreements, I think there's some work that needs to be
8 done there.

9 And I think -- and I think the last thing is
10 breaking down, in those -- in those last few areas
11 within the Department, this idea that we can do things
12 the old way, and all we need are technicians what --
13 the bare minimum that's required under the law, and
14 that will suffice for protecting privacy.

15 Those are the things that come to mind that
16 need to be addressed in the next -- in the next
17 administration.

18 MS. SOTTO: Anyone else?

19 [No response.]

20 MS. SOTTO: All right.

21 Hugo, on behalf of the committee and myself,
22 I want to thank you deeply for your years of service,

1 not only as Chief Privacy Officer and Chief FOIA
2 Officer, but your years prior to that, as well, for
3 DHS. You do have the most fabulous staff, incredibly
4 talented people, people who feel privacy in their
5 bones, and live and breathe it 24/7, as I know you do,
6 and we are very grateful for your leadership. Thank
7 you very much.

8 MR. TEUFEL: Well, thank you very much. It's
9 been the best job of my life to date. Don't know how
10 it can be beat, but it's been a fabulous, fabulous two
11 and a half years, and I want to thank you all for your
12 service on this committee. And wherever I may be next,
13 I hope to be working with all of you in some other
14 capacity. So, thank you all for your service.

15 MS. SOTTO: And next, we'll hear from Becky
16 Richards. Becky is the Director of Privacy Compliance
17 in the Privacy Office.

18 Thank you, Becky.

19

20

21

22

1 DHS LEGACY SORN PROJECT

2 MS. RICHARDS: Good morning. Is this on?

3 It's on? Okay. Pull it over close? I tend not to
4 have a problem speaking loudly.

5 So, I'm the technician out there, I guess. I
6 am going to talk to you for a few minutes about our
7 Legacy SORN Project, which has actually been a whole
8 lot of work and, I think, has been very important for
9 the Department, as administrative as it otherwise may
10 sound.

11 So, you know, System of Records Notices under
12 the Privacy Act, you know, was written in 1974, not
13 exactly the most exciting activity one can think about.
14 But, ultimately the Systems of Records Notice, or the
15 SORN, is a very important document. It's what we get
16 sued about, it's what people actually have their rights
17 for. It's things that -- you know, you can get civil
18 and criminal penalties as an employee if you aren't
19 doing it properly. It's -- you know, when there are
20 privacy incidents, this is what you go back to. So,
21 it's a fundamental part of how we do privacy at the
22 Department. And having all of these old System of

1 Records Notices sort of hanging around, that were, in
2 large part, unreadable, were under former authorities,
3 and didn't say a whole lot, we really worked to try and
4 improve the notice within the confines of what the
5 Privacy Act required us to do.

6 And so, while, yes, it's somewhat of an
7 administrative activity, as I know Joanne was
8 mentioning to me yesterday, it's been a really
9 important activity, from a number of perspectives.

10 We reviewed all 208 of these lovely System of
11 Records Notices. They came from Treasury, Department
12 of Energy, old INS, FEMA. And they were clearly
13 written by people who didn't necessarily know what the
14 systems were doing, didn't necessarily think much about
15 what they were collecting, and provided a minimal
16 amount of actual information about what they were
17 doing. And what we did is, we took a systematic
18 approach to every single one of these notices, and
19 reviewed them, to identify what at the Department we
20 needed. So, what are the basic functions that a
21 Department does, even from its employee perspective?
22 So, you know, time and attendance, how do you deal with

1 that? What information are you collecting? So, we
2 went through and basically started out by looking at,
3 What does a Department need? And we came up with about
4 24 System of Records Notices that encompass probably 50
5 percent of those SORNs, because they were just
6 administrative functions that we did at the Department.

7 And so, we created a consistency across the
8 Department that said, "This is how we're going to
9 handle it, this is when you can share it, this is what
10 we're collecting." And it took a great deal of effort
11 and much more time than I ever expected, because we had
12 to, not only get clearance through headquarters level,
13 you then had to go down to all the components, and you
14 had to make sure that they matched what the components
15 were doing. And it was -- I think it was a real
16 learning experience and educational experience; a
17 learning experience from our office and an educational
18 experience from the components' and from the
19 headquarters of -- "Oh, here's these privacy people,
20 they're coming back and asking us to review yet another
21 document. Ha. How does our information actually flow?
22 Ha. What do we actually do? How long do we really

1 need it?" And so, while, yes, it's somewhat of an
2 administrative function, it's an educational
3 opportunity, as well.

4 And so, we went through that process, and it
5 took a long time, a really, really long time. It took
6 15 months. And hopefully by Friday everything will be
7 done, as Hugo says. And if it isn't, I'm probably in
8 trouble.

9 But, we've had myself and two contractors
10 review every single one of these and go through. And
11 basically what we found was a couple of things. The
12 previous SORNs never had a purpose statement. Heaven
13 forbid you should read some of these SORNs. You don't
14 know what they're collecting. And I've now read
15 hundreds, if not thousands, of these things, and I
16 couldn't figure out what they were trying to tell me
17 they did. So, you'd send them down, and they'd say --
18 "What are you trying to say here?" And so, I am
19 hopeful that, you know, because we've had a systematic
20 approach, every one of the System of Records Notices
21 looks the same, our routine uses are, across the board,
22 pretty much the same, fairly consistent, and/or, you

1 know, you only add or subtract what you need or don't
2 need, but they're the same routine, you know, so you
3 don't see it's some little language here and some
4 little different language over here.

5 We looked at all the authorities to make sure
6 that they were actually accurate. And the authorities
7 was a sort of fascinating activity, in finding that
8 some of those authorities didn't exist anymore, that
9 they didn't actually do those things anymore. But,
10 going through and cleaning those things up. Again,
11 we're going to get sued over these things at some
12 point, maybe, and so, you want to make sure they're
13 accurate.

14 The categories of records and categories of
15 individuals were equally important. You know, what are
16 you collecting, who are you doing it on? And then, we
17 just tried to really just increase the detail in the
18 System of Records Notice. Yes, it's still a legal
19 document. Yes, it's not really user-friendly or -- you
20 know. But, I think that the SORNs that you see today,
21 if you go back, you know, even five years, are much
22 better, they actually provide some level of notice. If

1 you, you know, sort of, have a little bit of idea of
2 what you're looking for, you can find it. I think you
3 also see that in some of the responses. We're actually
4 getting public comments on our System of Records
5 Notices. Nobody every did, before we published the
6 Automated Targeting System, very many. Nobody really
7 knew that we published these things, there wasn't a lot
8 of public outcry. So, I think that that's been --

9 And then, the other thing was, you know, we
10 looked at them to update the retention schedule. At
11 the end of the day, if you're not maintaining the
12 information, the -- for a long period of time -- your
13 privacy concerns start to go away. So, you can't share
14 it for some mission-creep issue if you don't -- only
15 retain it for a couple of years.

16 So, we went through this. We reviewed all of
17 them, as well, updated the exemptions, and finished
18 that publishing. And so, basically, at the end of the
19 day, we'll have 24 DHS-wide System of Records Notices.
20 They're all up on our website. And then, we have a
21 bunch of these component-specific. And what I am
22 hopeful this will do is, then now it puts us in a

1 position that we're able to, bi-annually, actually do
2 the reviews that are required. We're actually able to,
3 you know, address issues that come through. And we're
4 not working off of a backlog. Because at the same time
5 that we were doing this SORN project, we improved our
6 FISMA numbers. FISMA is the Federal Information
7 Security Management Act. And we're required, on an --
8 quarterly and annual basis, to report to OMB how many
9 PIAs have we done on the IT systems that require PIAs,
10 how many System of Records Notices. And so, as, I
11 think, John reported, or maybe it was Hugo, in
12 September, we improved our numbers from 26 percent. As
13 of our December number, it's now at 55 percent of all
14 PIAs that are required for an IT system are done. And
15 that number will continue to go up, so that when the
16 new administration comes in, there isn't this backlog
17 of what needs to be done, we're able to actively engage
18 on a lot of those activities up front so that we're not
19 doing fire drills and we're not looking at some of
20 those issues.

21 Let's see, during the last year, our group
22 also published System of Records Notice guidance, so

1 that, going forward, as new programs come through, they
2 know how to write their SORN, they know what the basic
3 routine uses are, should be, and learn from that. We
4 did a bunch of training as it relates to Privacy Impact
5 Assessments, so that that training is now at the --
6 again, it's at the bureaucratic level, in the best
7 sense of the word "bureaucrat," so that you're really,
8 from the ground up, incorporating privacy into what we
9 do every single day, so that it's not just somebody on
10 high saying, "Thou shalt do privacy," it's the people
11 at the bottom who are, in some cases, checking a box,
12 but then, doing that check-box, they are making sure
13 that there is privacy there, they're making sure the
14 basic functionalities are described and that there's
15 transparency of the system.

16 So, I'm excited for the -- for what we are to
17 come after Friday, when I stop having to read SORNs.

18 [Laughter.]

19 MS. RICHARDS: And there have been projects
20 that have been put somewhat on hold as we go through
21 this process. But, it's been -- it's been an important
22 aspect of really getting one DHS, one coherent

1 organization, that isn't -- that really knows it. And
2 I think our next steps are also now to work with
3 Catherine's group and the FOIA and Privacy Act
4 disclosure side to make sure that the notices that are
5 out there are what we're giving back to people when
6 they request it, so that they're getting the redress
7 that they need or they're getting access to the
8 information. And that's going to be, sort of, the next
9 phase of this process.

10 So, that's about all I have, unless you all
11 have questions.

12 MS. SOTTO: Thank you very much, Becky.

13 Joanne?

14 MS. McNABB: I apologize for underestimating
15 the educational value of going through this laborious
16 process, and I congratulate you on your huge
17 accomplishment.

18 MS. RICHARDS: Thank you. It was not quite
19 as -- it was quite evil, but --

20 [Laughter.]

21 MS. RICHARDS: -- it's done now.

22 MS. SOTTO: Ramon, please.

1 DR. BARQUIN: In the context of some of the
2 things that are going on with SOAs, with Service-
3 Oriented Architectures, how are you storing the SORNs,
4 given that there must be a wealth of information on
5 data elements collected and things like them in them
6 that could be helpful?

7 MS. RICHARDS: So, we have taken the
8 approach, for the System of Records Notice, to not look
9 at it as IT-centric. In other words, we're looking at
10 it from a collection of information, where the
11 categories of records, categories of individuals and
12 purposes, are basically the same. And so, what you end
13 up doing is having an IT system that may actually
14 implicate four or five different System of Records
15 Notices with different aspects of it. And part of our
16 PIA process -- you can actually see a couple of our
17 examples of this; for example, we have the Enterprise
18 Service Bus, which then allowed us to pull a whole
19 bunch of different from a -- one -- and show it up on
20 one screen. One of the aspects that we've done with
21 that is, the PIA goes through and basically verifies
22 that the information collected is for the same -- is

1 for a compatible purpose, that it -- you know, that
2 everything meets the same requirements and we're
3 transparent about how that is. So, you can see those
4 PIAs on our Web site. And there have been instances
5 where people have wanted to add in systems, but the
6 information is not really compatible or similar to what
7 they're wanting to do, and there's been a lot of back-
8 and-forth as to what -- how you handle those types of
9 things.

10 The other part of that process has been --
11 we've seen different IT functionality, and we found
12 that there are some we like better than others, from a
13 privacy perspective. So, for example, when you do a
14 person-centric query related to -- and it's going to go
15 to seven different System of Records Notices or eight
16 different IT systems, we want to make sure it's clear
17 that you know what system it's coming back from. So,
18 if it comes up and says "Becky Richards," and it
19 doesn't just outright say, "This is the information,"
20 but, rather, says, "Here's the information from these
21 six different places," so that you can go back and say,
22 "Ha, the information isn't quite the same when I look

1 it, because my middle initial -- the person's middle
2 initial" -- so, you can identify and actually improve
3 the data integrity.

4 So, in some cases, what we've seen,
5 particularly USCIS, who's embraced this because they
6 have both -- they have some data-integrity issues mixed
7 with very legacy systems that don't do a whole lot of
8 anything beyond, you know, you put the name in, and it
9 comes back up. But we've seen some real improvements,
10 actually, in our ability to make changes through the
11 system, so that if you, when you pull that record up
12 because somebody -- you know, somebody isn't getting a
13 benefit, and it's because there was some problem
14 somewhere in there, they can go back and find that.
15 And we've preferred that model fairly heavily over
16 something that just brings up the information and you
17 don't know where it came from.

18 MS. SOTTO: Any other questions for Becky?

19 [No response.]

20 MS. SOTTO: All right.

21 Thank you very much, Becky.

22 MS. RICHARDS: Thank you.

1 MS. SOTTO: Catherine Papoi, would you join
2 us? Thank you.

3 Catherine is the Deputy Chief FOIA Officer,
4 and is also a member of the transition team. So we're
5 very interested in hearing from you, Catherine, to help
6 us understand how the transition is going and what the
7 issues are that on the front burner for the transition
8 team.

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 PRESIDENTIAL TRANSITION - DHS PERSPECTIVE

2 MS. PAPOI: Certainly. Thank you.

3 Let me start by saying it was extremely
4 generous of Hugo to give me a 100-percent detail to the
5 core presidential transition team at headquarters.

6 Some background. Congress, several years
7 ago, expressed extreme concern over the transition at
8 DHS, being that this would be our first transition.

9 And although the other 14 agencies or departments had
10 gone through transitions numerous times, this would be
11 a first for DHS.

12 That being said, they appointed Under
13 Secretary Elaine Duke as the lead on the DHS transition
14 effort. Elaine Duke then asked Admiral John Acton to
15 step up as the director of the transition effort.

16 Admiral Acton then hand-selected a cadre of senior
17 careerists at DHS to assist him in the transition team.
18 And there are approximately -- about 15 of us now
19 working on this effort.

20 And I started, let's see, in October, and was
21 way behind the eight ball as the rest of the careerists
22 had been working with Admiral Acton for approximately nine

1 months in teeing up many of the pieces and putting them
2 into place on several different levels.

3 There was internal preparation that was
4 necessary. Essentially, we wanted to make sure that
5 there were training and exercises in place for all of
6 the senior careerists in every single office at DHS,
7 those people that would be stepping into the place of
8 those appointees as they're leaving. So, for instance,
9 within the Privacy Office, John Kropf and myself would
10 be stepping up to take charge, should some sort of an
11 emergent situation occur in the interim, Hugo leaving
12 and the next person appointed to take over as Chief
13 Privacy and Chief FOIA Officer.

14 In addition to participating in these
15 training activities, we've developed briefing materials
16 internally to brief not only the incoming -- new
17 incoming administration, but also the -- what has been
18 coined the "Parachute Team," but the Obama's -- Obama's
19 camp has coined themselves the "Agency Review Team."
20 And so, we termed the "ART" members that descended upon
21 DHS. Let's see, it was October -- or, I'm sorry,
22 November 17th. We have 38 ART members that are at DHS,

1 and they are looking at all aspects of the Department.

2 The Department, overall, has received
3 extremely positive response to its briefings on the
4 transition efforts. We've briefed the House and Senate
5 Homeland Security Committees, GAO, OMB, the White House
6 Homeland Security Council, and they have all said the
7 DHS transition plan has really been touted as best
8 practice for the other Departments to consider.

9 Because of the initial concern from Congress, we really
10 stepped up to the plate and made sure that we were not
11 only prepared, but we were overly prepared for any sort
12 of instance that could -- that could come our way.

13 Once the ART members arrived, on November
14 17th, we only had about a day -- a day's notice as to
15 who those members would be. And I brought with me the
16 names of some -- and you may recognize some of these
17 names. Some of them are -- have experience on the
18 Hill, prior experience within the Department of
19 Homeland Security or within the intelligence field.
20 For example, the lead of the ART team -- actually, it's
21 a two-person lead -- it's Rand Beers, and he, from '02
22 to '03, was Special Assistant to the President and

1 Senior Director for Combating Terrorism. In addition,
2 his co-lead is Clark Ervin, who was the first Inspector
3 General at DHS. And those two are heading up the team.

4 Interestingly, Randy Beardsworth, who was
5 previously with DHS, is on the team. Jane Bullock, who
6 served as Chief of Staff to FEMA from '92 to 2000, is
7 on the team.

8 Juliette Kayyem is on the team. And some of
9 you may know her. She has a high interest in privacy,
10 and, in fact, she met with Hugo, John Kropf, Toby
11 Levin, and myself last week to talk specifically about
12 the Privacy Office, and the majority of the time we
13 focused on privacy issues. She served as legal advisor
14 to Attorney Janet Reno, and she worked on a variety of
15 national security and terrorism cases, but privacy is
16 near and dear to her heart.

17 Paul Kurtz is focusing on cyber issues.
18 David Martin, who is General Counsel at INS, and Gening
19 Liao, is also focusing on immigration-related issues.
20 We have Nelson Peacock, counsel to Senator Lieberman
21 and the Senate Judiciary Committee since May of '05.
22 Sue Ramanathan -- I always have trouble with her name

1 -- she was Chief Counsel and Deputy Staff Director for
2 the House Homeland Security Committee. And we have Bev
3 Pheto, who was the subcommittee clerk to the House
4 Committee on Appropriations for Subcommittee on
5 Homeland Security.

6 So, that gives you a flavor of some of the
7 members. Very diverse, extremely knowledgeable in
8 their areas. And what they have requested are a series
9 of briefings on particular topics. They've requested
10 site visits to particular components. And they've
11 requested specific documents that they know exist
12 within the Department. And all of this is in
13 preparation for a document they need to prepare and
14 deliver to Obama's team on the 19th of December. So,
15 it's a fairly short fuse for them. For example, I've
16 been heading up the effort for the request for
17 information and briefings, and the weekly agendas are
18 packed. They are in briefings from about 7:30 a.m. til
19 about 7 p.m. every night. And so, they really are
20 doing their intense research.

21 As I said, Juliette Kayyem has a high interest
22 in privacy, and we actually offered her a site visit to

1 our offices, if she was so interested. We haven't
2 heard back on whether she'll take us up on that or not.

3 As it relates to teeing up issues for the
4 next administration, that's the other piece that our
5 transition team is focusing upon. And we have the
6 onboarding tiger team, per se. And essentially, when
7 they prospective appointees come in, they will
8 essentially go through the duplicate briefings that the
9 ART members have gone through, and the Council for
10 Excellence in Government is assisting in developing
11 exercises for the new appointees so that they can go
12 through tabletop exercises and be prepared, should,
13 again, an emergent situation occur, you know, the first
14 day they're in office, so that they're not left
15 wondering what to do.

16 We've developed, at the headquarters level, a
17 30-60-90-day priority list. And that was presented to
18 the transition team, the ART team members. That 30-60-
19 90-day list includes all issues or determinations that
20 will be made or need to be addressed within the first
21 -- you know, within the first 100 days in office.

22 The binder for the incoming appointees

1 includes issue papers on every single office at DHS, on
2 every single program within each office at DHS. It's
3 extremely comprehensive. It was a heavy lift. But, it
4 will be very useful to the incoming administration.

5 And last but not least, we -- obviously,
6 yesterday, the official announcement was made of the
7 new proposed Secretary, Governor Napolitano, and we've
8 already been in contact with her staff, and we
9 anticipate meeting with members of her staff with --
10 probably this week. So, she's being extremely
11 proactive in getting a handle on all of the issues and
12 pending determinations that she needs to make once she
13 is confirmed.

14 So, that gives you a general overview of the
15 transition. It's been very interesting and
16 enlightening. I've been sitting in on many of the
17 briefs for all of the various components of DHS, and
18 I've learned more about DHS in the last two weeks than I
19 have in the last three and a half years. But, it's a
20 fantastic opportunity.

21 Are there any questions on the transition?

22 [No response.]

1 MS. SOTTO: No questions.

2 MS. PAPOI: Wow.

3 MS. SOTTO: All right. I will -- I will ask
4 one, then -- and then, John, you're up next.

5 Juliette Kayyem --

6 MS. PAPOI: Yes.

7 MS. SOTTO: -- has expressed interest in the
8 Privacy Office. That's terrific. Can you give us a
9 quick rundown of what recommendations you've made to
10 her, how to -- how to keep in place what I think is the
11 strongest privacy office in the Federal Government, and
12 how to enhance its ability to move forward effectively?
13 I'm also interested in your sense of how immersed she
14 is in privacy and what kinds of -- what her -- what her
15 knowledge is right now and what her knowledge -- how
16 her knowledge has been enhanced in what she might be
17 recommending to her team?

18 MS. PAPOI: Absolutely. I'm going to work
19 backwards, in terms of your questions.

20 Her knowledge -- it's been a quick study for
21 her. I mean, she has privacy experience in her
22 background; however, as she put it, within the last

1 year or so she's been somewhat removed. And so, she
2 asked for many reference materials and really had to
3 spin up quickly on all of the issues at hand. So, I
4 think she's very knowledgeable at this point,
5 especially as it relates to the privacy issues that are
6 applicable to homeland security.

7 As it relates to what we have recommended or
8 pointed out as concerns or recommendations going
9 forward with the Privacy Office, we suggested that it
10 was extremely important that we remain highly visible
11 within the Department. And the transition team has
12 expressed concern over the number of small direct-
13 report offices. She specifically asked us why we felt
14 it was important that we remain as a direct-report.
15 And, honestly, it speaks for itself. I mean, we -- to
16 keep the visibility, to maintain the appearance of, you
17 know, autonomy in the policy realm, we need to be
18 responsive right to the Secretary, we need to have that
19 direct line. And if we were to be buried within
20 another component -- say, Policy -- I think we would
21 lose a lot of efficacy. And she seemed to understand
22 that completely.

1 In addition, we recommended that the
2 leadership support, the privacy initiatives, make sure
3 that it's top-down support. If we don't have that top-
4 down support, then it -- we spend the majority of our
5 time with internal battles, and you end up wasting a
6 lot of energy on those efforts.

7 So, after making those recommendations, we
8 also pointed out that, you know, Becky and Toby and all
9 of the members of our staff that have done such an
10 outstanding job and really do serve as the, you know,
11 perfect paradigm for how a privacy office should be
12 run, you know, those pieces need to be recognized by
13 the incoming administration as -- you know, we have a
14 very significant and important office mission, and that
15 we deserve the support of the new administration, and
16 we hope that they understand that we need to remain
17 independent of one of the larger offices, and
18 consolidate will not further, you know, or enhance our
19 efforts.

20 MS. SOTTO: We certainly, I think, uniformly
21 support everything you've just said and what you've
22 conveyed to Juliette, and I would offer members of this

1 committee to speak with her. We would be glad to do
2 so, if that would be helpful to her. I think we have
3 some pretty strong views around this table about the
4 independence of the Privacy Office.

5 And, Catherine, I would urge you to stick
6 around, if you can, because we're going to be having a
7 discussion amongst ourselves, publicly, about some
8 issues that we see as those that ought to rise to the
9 top for the next administration. And those might be
10 interesting issues for you to convey to Juliette or
11 others, and certainly we would be glad to convey them
12 ourselves, if you think that would be useful.

13 MS. PAPOI: I -- unfortunately, I have a GAO
14 exit interview, not one of -- top of my list for fun.
15 But, what I would ask, if someone could send me, e-mail
16 me, those issues, I would be more than happy to convey
17 those to Juliette and others on the team that have
18 expressed interest in either privacy or consolidation
19 of the independent smaller direct-report offices.
20 Because we do -- that is something that's dear to our
21 heart, and we want to make sure that the new
22 administration understands this.

1 Now, understanding that, the incoming
2 Secretary, one of the priorities is on the immigration
3 issue. That's near and dear to her heart. And a piece
4 of that will obviously involve privacy. And I think if
5 we can tie those two pieces together and approach it as
6 such, I think that will raise our visibility to the new
7 Secretary. So --

8 MS. SOTTO: Thank you.

9 We are -- we are planning to have a small
10 subcommittee of the larger committee address transition
11 issues and write something, so we'll be --

12 MS. PAPOI: Fabulous.

13 MS. SOTTO: -- sure to get that to you --

14 MS. PAPOI: That's great.

15 MS. SOTTO: -- as soon as we can, because I
16 knew time is of the essence.

17 MS. PAPOI: It is.

18 MS. SOTTO: Okay.

19 MS. PAPOI: It is. That's fantastic. Thank
20 you.

21 MS. SOTTO: John Sabo?

22 MR. SABO: Just a quick -- two quick

1 comments. One, on the direct reports. Am I mistaken,
2 but the legislation -- the Homeland Security Act,
3 doesn't it -- doesn't it require the Privacy Office to
4 report to the Secretary?

5 MS. PAPOI: It does. However, if they
6 decided to put us within another --

7 MR. SABO: Oh, I see.

8 MS. PAPOI: -- direct-report office --

9 MR. SABO: I see what you're saying.

10 MS. PAPOI: -- it -- I don't -- I -- you
11 know, I'm --

12 MR. SABO: Okay, no, I --

13 MS. PAPOI: -- not a practicing lawyer, but
14 they could, maybe, make the argument that that would
15 suffice as a direct-report. Again, just as they've
16 consolidated the Chief Privacy Officer with the Chief
17 FOIA Officer --

18 MR. SABO: All right.

19 MS. PAPOI: -- you know, it is still a --
20 deemed a direct-report. So --

21 MR. SABO: The other quick question, just to
22 follow up on Lisa's comment, has the transition team at

1 all met with, or requested to meet with, any of the DHS
2 Advisory Committee chairs or vice chairs?

3 MS. PAPOI: They have not --

4 MR. SABO: Okay.

5 MS. PAPOI: -- yet. And I believe -- it's
6 not that it's not on their radar, I think it's simply
7 the overwhelming amount of information that they are
8 trying to absorb within their, you know, month --

9 MR. SABO: Right.

10 MS. PAPOI: -- that they have.

11 MR. SABO: Okay.

12 MS. PAPOI: Yeah. But, I would anticipate
13 that the team coming in, of appointees, we're actually
14 expecting kind of an interim team, kind of the
15 designees of the prospective appointees to come in,
16 sort of teeing things up even further for the incoming
17 administration. And that might be something where they
18 delve a little deeper so they can get some more
19 opinions from those that are not necessarily ensconced
20 within DHS.

21 This team, interestingly, has -- partially
22 because some of the members are prior DHS employees --

1 very early on, made it -- made us aware that they
2 intended to talk to many of the senior careerists and
3 not necessarily only speak with the political
4 appointees, because they really wanted to get -- to get
5 down into the weeds and not necessarily just hear what
6 is being touted as the -- as the line, per se.

7 MS. SOTTO: Other questions?

8 Yes. Please, Dan.

9 MR. CAPRIO: Thanks, Catherine.

10 Just had a quick question, to follow up on
11 what you, I think, just alluded to. But, you had
12 mentioned, kind of, the 30-60-90-day issue spotting,
13 and then the possibility of sort of an interim
14 transition team, if you will. Do you have any sense or
15 a timeline of -- you know, as the Secretary-designate,
16 comes in and is confirmed -- as she gets her team in
17 place, you know, the -- her management team -- the
18 deputy secretary, under secretary, assistant
19 secretaries, and -- I mean, you see where I'm going
20 with this -- it's sort of, you know, when do we get
21 down to the point of -- you know, because you -- it's a
22 layered approach, when we get to the Privacy Office.

1 MS. PAPOI: Yeah, like, full-fledged -- when
2 are we on, full-fledged --

3 MR. SABO: Right.

4 MS. PAPOI: -- everyone's covered? Well, we
5 have, I think, currently -- let's see, here -- I want
6 to say, at headquarters level alone, let's see, here,
7 80-some-odd appointee positions. I would say this,
8 though. From what I've seen of the administration,
9 thus far, they move quickly. Very quickly. And being
10 that we heard -- within an hour of the official
11 announcement that Governor Napolitano was coming in, we
12 heard from her staff, I anticipate that she will
13 probably have all of her staffing set pretty much upon
14 her confirmation. I -- and, again, this is my personal
15 opinion, but they move fast. Very quickly. And, as
16 you know, the President-elect promised that, that he
17 intended to move quickly. And so, I do not see the
18 Privacy Office languishing without an appointee for
19 very long. I do anticipate that we will be -- everyone
20 will be up and staffed, if not, like, as I said, upon
21 her confirmation, soon thereafter.

22 MS. SOTTO: More questions for Catherine?

1 [No response.]

2 MS. SOTTO: Okay.

3 Catherine, again, just to reiterate, we are
4 here, willing to assist in any way that we can, so
5 please take advantage of the incredible expertise
6 around this table. What a group of people you have
7 access to here; and we are here, and ready and willing
8 to assist.

9 MS. PAPOI: Fabulous.

10 MS. SOTTO: Thank you.

11 MS. PAPOI: And if any of you have, as I
12 said, recommendations, et cetera, please, please e-mail
13 me. Ken can give you all of my contact information,
14 and I am more than willing to pass that on to the team
15 members as an offer either to meet or as
16 recommendations from the Advisory Committee. So, I
17 thank you.

18 MS. SOTTO: Thank you very much.

19 Okay, we are -- we had a little bit of change
20 in agenda, because some of the afternoon speakers
21 needed to shift around their schedules a little bit, so
22 we're going to turn to subcommittee updates now. So, I

1 hope you all don't mind if I call on you before lunch
2 instead of after lunch to give subcommittee updates.

3 The first subcommittee I'd like to turn to is
4 the Data Integrity and Information Protection
5 Committee. And Ramon Barquin, who is the chair of that
6 subcommittee, is going to give us a report.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 Would Joanne McNabb give us a report on the
2 Privacy Architecture Subcommittee please?

3 MS. McNABB: Yeah.

4 In our continuing efforts to build privacy
5 considerations into the procedure for awarding grants
6 to states, we are going to be having a teleconferencing
7 meeting with some of the Privacy Office staff and the
8 Grants Office staff, and keep moving toward that.

9 MS. SOTTO: How has that process been going?
10 You've been working on that for a little while.

11 MS. McNABB: Slowly.

12 MS. SOTTO: All right. I would -- I would
13 urge you, if you need more assistance, to get with
14 folks in the Privacy Office and --

15 MS. McNABB: The Privacy Office have -- are
16 being very helpful on this, and we're hopeful that
17 we're going to come up with something good.

18 MS. SOTTO: Thank you very much, Joanne.

19 David Hoffman and Richard Purcell are co-
20 chairs of the Data Acquisition and Use Subcommittee.
21 Which of you is interested? Thank you, Richard.

22 MR. PURCELL: Thank you, Lisa.

1 As all Federal agencies are concerned, DHS is
2 vitally concerned with information-sharing environment
3 issues. They're permeating all the Federal Government
4 right now. In support of the Privacy Office's request
5 for an analysis from our subcommittee and guidance for
6 improving the Department's capacity, readiness, and
7 capabilities for being -- providing leadership in the
8 information-sharing environment, we're working on --
9 we're working on that guidance.

10 We've received a variety of inputs from both
11 the Privacy Office and from components regarding the
12 information-sharing and access-agreement protocols,
13 Memorandum of Understanding, and Computer Matching
14 Agreements. We've been working for a year now
15 gathering materials from the OIG, from FEMA, from a
16 variety of sources within and outside the Department.
17 And we're -- now are committed to an analysis and the
18 creation of guidelines that'll create a set of uniform
19 policies and practices for respecting and protecting
20 personal information within the dynamics of an
21 information-sharing environment. This includes
22 leadership within our subcommittee.

1 Kirk Herath will be leading an effort to
2 define the sharing agreement requirements for privacy
3 and data protection. Ana Anton will be leading the
4 development of the templates for these agreements, with
5 illustrative examples to provide context. Certainly,
6 the contexts for these agreements is going to differ,
7 depending on the component, given the wide range of
8 components within the Department. And then, Dan Caprio
9 will be developing -- leading the effort to develop and
10 deploy communication protocols and programs to promote
11 a comprehensive understanding of the implications of
12 implementing these agreements within the subject
13 components themselves.

14 So, it's a thorough look at how we can create
15 a uniform standard of policies and supporting practices
16 and communications for awareness and education for
17 these sharing agreements so that the intention of the
18 agreements are carried out, specifically, within
19 limits, but not as barriers, but rather as facilitators
20 of the component and the Department's business.

21 MS. SOTTO: Do you intend to issue a paper?

22 MR. PURCELL: We do. We hope, by the next --

1 in the next 60 days, to have something for this
2 committee's review, and then we hope to then promote it
3 to the whole committee.

4 MS. SOTTO: Excellent. Thank you very much,
5 Richard.

6 I'd like to turn the floor over to John Sabo.
7 John has been leading the charge for an ad hoc
8 subcommittee to look at certain privacy issues
9 associated with the E-Verify program.

10 So, John, if you could talk to us a little
11 bit about the paper that we are looking to issue today.

12 MR. SABO: Yes, thank you.

13 The purpose -- and I think I asked all the
14 committee members earlier to review the draft that is
15 in our packets and has been distributed. This draft is
16 something I will walk through and then take any
17 questions on. There may be some issues, or not, that
18 you might want to raise. And our goal would be to have
19 a vote of the full committee on this draft document so
20 that we can use this formal meeting to respond to the
21 request for guidance on the E-Verify program.

22 So, this particular document is a -- a narrow

1 response to a fairly narrow question raised by the
2 Privacy Office to the committee. We were tasked,
3 September 15th [inaudible] via e-mail, to basically
4 review certain characteristics of the E-Verify program
5 related to authentication and to provide some
6 recommendations on addressing the problems. And you
7 might recall that -- I think, in two prior DPIAC
8 meetings, where we had input and testimony from the
9 office in charge of E-Verify, that there was a -- a
10 number of questions arose, and we responded to somewhat
11 -- in some cases, alarmingly -- about the
12 authentication protocols used for E-Verify, and, in
13 response to that, the tasking, on September 15th, to
14 the committee.

15 So, before I move into this, I do want to say
16 that, at the very end of the document we make a comment
17 that the E-Verify -- the committee, in fact, looks
18 forward to further dialogue in the program. The
19 program itself has been very controversial. We don't
20 get into that issue. We have not been -- it's not our
21 purview, we've not been tasked to assess the efficacy
22 of the E-Verify program as a governmental program.

1 It's a congressional mandate. And, as you know now,
2 there's an executive order from the President which
3 requires that E-Verify be used by Federal contractors
4 and subcontractors. So, the scope of the program, by
5 executive order, is being extended. We don't get into
6 those issues. We were asked, and our charge is, to
7 look at the data privacy and associated security and
8 data integrity issues around the program. So, I just
9 wanted to make that clear, that there are those who see
10 issues with the overall program, and that's not what
11 we're focusing on.

12 So, let me just walk through this quickly and
13 then take any questions on it.

14 The draft references the task that we were
15 given. DHS, the Verification Division within CIS, has
16 established an E-Verify employer registration business
17 process re-engineering program. They have a team,
18 called the BPR Identity Assurance Design Team, that is
19 focusing on improvements to the authentication
20 protocols for E-Verify. As you might recall, E-Verify,
21 as a program -- if I can pull it up -- we had a final
22 rule issued in August, and that final rule put in place

1 provisions related to the use of the program by Federal
2 contractors -- subcontractors. And that talks a little
3 bit about how the system works.

4 And essentially, there's a query, which goes
5 into a -- the E-Verify system. The query goes off to a
6 USCIS database to look at immigration data, and the
7 query goes off to the Social Security Administration to
8 get a response to -- a match of the name, the Social
9 Security number, and the date of birth of the employee.
10 The employer signs up for these -- the system in a
11 completely online environment. And there is no
12 structure in place to register the identity of
13 employers, externally; basically, it's an online
14 environment, and there's a attestation that the
15 employer is really an employer and that the data
16 they're sending in the -- you know, they're willing to
17 -- they agree to all the conditions of -- terms and
18 conditions of use of the application. But there's no
19 out-of-band verification of the employer, per se, and
20 that is one of the core issues of E-Verify that we saw.
21 And one of the dangers that's inherent in it is that it
22 can be -- there's a -- it's a basically a

1 vulnerability, it's a security vulnerability. An
2 attacker can make use of the E-Verify system, claim to
3 be an employer, and use it to begin searching for
4 matches of an SSN, a name, and a date of birth. And,
5 you know, that is a huge security vulnerability,
6 because it exposes -- (a) it exposes confidential
7 Privacy Act information to confirmation or
8 nonconfirmation by bad actors, and that could be used
9 in a whole number of ways.

10 So, we saw a security vulnerability, and the
11 team has requested that we basically take a look at
12 options for addressing that particular set of issues
13 and any others related to authentication.

14 So, what we've done in this paper is, we've
15 outlined the issue, we've -- the scope of the issue,
16 and we put together a committee. We had
17 teleconferences with the BPR team members and with the
18 Social Security Administration, the Privacy Office, and
19 we've proposed a number of ways to approach this issue.

20 First of all, just walking through this
21 quickly, there is a well-documented set of standards
22 and guidance from OMB, and from NIST in particular,

1 related to assessing the risk of online applications,
2 the security risks. And again, security is a key
3 component of data privacy. And we made the point of
4 including a number of those key documents in this
5 response, because, although these should be known to
6 the agency -- the Department CISO and the agencies'
7 security people, it wasn't clear to us that the
8 Identity Assurance Team had staff within the team which
9 -- who were familiar with the -- this guidance and
10 these requirements. And basically, it's a subset of
11 the whole NIST family of guidance, which is mandated
12 for use by Federal agencies, including the Federal
13 Information Processing Standards and special
14 publications.

15 So, we recommend that, and we particularly
16 recommend that the design team if -- be expanded to
17 include a security professional familiar with these
18 standards and a member of the Verification Division
19 Privacy Office to ensure that these documents are
20 properly considered in building the system.

21 A second point we note is that OMB M-04-04,
22 which is the authentication guidelines -- a lot of

1 acronyms -- basically, there's an interesting comment
2 there, that one of the issues about expanding a system
3 which may have some fundamental authentication flaws is
4 that the tradeoff is, if we make it too difficult to
5 use, then it will cut down on usage. And OMB, in its
6 2003 guidance, essentially says that simply increasing
7 the size of the customer pool shouldn't be an offset to
8 increasing the risk associated with corrupting the
9 appropriate assurance levels. So, the OMB guidance
10 basically says, "You don't sacrifice security controls
11 in order to ensure more people can use the system," and
12 we wanted to point that out in this set of documents.

13 So, we offer a number of very specific
14 recommendations. First of all, we say the fundamental
15 starting point is to use the NIST guidance in assessing
16 the level of sensitivity, the appropriate selection of
17 controls, and the risk associated with the application.
18 And we point out that the Social Security
19 Administration has a -- an employer verification
20 system. Its purpose is not for employment eligibility,
21 but its purpose is to ensure that when an employer is
22 basically reporting wages for an employee, that they

1 are properly reporting the wages against a name and a
2 Social Security number. And in the Social Security
3 Administration system, it's basically providing the
4 same disclosure -- it's a yes or a no -- which is what
5 E-Verify does, for all practical purposes. So, in the
6 Social Security Administration's case, they use much
7 stronger level of security controls in order to
8 register, identify, authenticate both the employer as
9 well as the employee or the contractor working for that
10 employer who uses the system. The E-Verify system
11 doesn't come anywhere near the level of those controls,
12 and we point that out, and possibly the NIST guidance
13 can assist the agency in doing that.

14 The second recommendation is: explore options
15 for establishing an employer identification
16 authentication system modeled on SSA's employer
17 verification system specifically. And they use, for
18 example, an out-of-band mailing back to the employer,
19 which provides a code that is entered to allow the
20 employer to access the system. So, of course there is
21 additional cost and there's additional time lag, but
22 it's a stronger method of identification and

1 authentication.

2 The third recommendation is to identify and
3 authenticate all individual users of E-Verify -- that
4 is, all individual users, not simply the -- and name of
5 the employer, the employer EIN, but also all users of
6 the system, and that doesn't appear to be done today.

7 The fourth is to have legal counsel in DHS,
8 IRS, and the Social Security Administration explore
9 options whereby employers in use of the system, may
10 provide permission for the use of the EIN for E-Verify
11 purposes. One of the -- one of the obstacles that we
12 were informed of is that the Internal Revenue Code,
13 Section 6103, which is mandated for use by Social
14 Security, prohibits Social Security from allowing E-
15 Verify to use the EIN as a matching element in the
16 system. And this points to a problem we've talked
17 about before in the committee, where you have, you
18 know, one code in one agency, another system in another
19 agency, and a program that both use; and, in fact, you
20 can't -- you can't have one agency allowing another
21 agency to make use of the same controls, because of a
22 legislative obstacle or a regulatory obstacle. So, the

1 -- what we're suggesting is, let the legal counsels get
2 together and see if there are ways to, within the law,
3 make appropriate use of the EIN to help properly verify
4 the employer and the employee who may be using the
5 system on behalf of that employer.

6 This is sort of striking, because, in a way,
7 it's the same disclosure, and yet, a tool that's
8 available for SSA to screen the users of the system to
9 properly authenticate and identify them is not
10 available to the E-Verify system. It seems -- you
11 know, it just doesn't seem consistent with good
12 government practice. So, hence, our recommendation.

13 The fifth recommendation is to develop
14 alternative registration and authentication methods
15 that would reflect existing levels of trust associated
16 with types of employers or third-party service
17 providers, to enable better risk management. So, you
18 could have registration and identification processes
19 for large employers, for large contractors who service
20 large employers, which would differ from processes put
21 in place for, you know, an employer which only has two
22 or three employers, like a small company. And your

1 risk management processes would differ very -- you
2 know, based on the risk assessment against these types
3 of employers.

4 The sixth is to consider the use of
5 commercial information sources to verify the identity
6 of employers registering to access the system, and
7 establish agreements and processes with employers who
8 authorize certain employees or third parties to use E-
9 Verify.

10 The seventh is to implement audits and take
11 steps to penalize and publicize fraudulent uses of the
12 E-Verify system. We didn't necessarily have a strong
13 sense that there was a very robust auditing system in
14 place to monitor usage of the system, and that --
15 that's a very significant piece of security controls.

16 So, finally, our last comment was the -- a
17 notion that adequate privacy and security controls will
18 require an investment in the E-Verify program. If
19 you're going to put in place and mandate the use of an
20 elaborate employment eligibility program that relies on
21 employer/employee authentication, then you've got to
22 fund it properly and put the right security and privacy

1 and data integrity controls in place. And again, going
2 back to the OMB guidance, you can't sacrifice -- you
3 know, you can't sacrifice security and privacy simply
4 to say, "Well, it's too expensive to do it properly."
5 You know, we feel that the right controls, if they
6 require additional investments, they need to have the
7 investments.

8 And finally, as I said, we look forward to
9 any further -- further dialogue with the BPR team and
10 the Privacy Office on other issues associated with E-
11 Verify that were not within scope of the tasking.

12 So, having elaborately and laboriously walked
13 through the memo and bored everybody, why don't we see
14 if there are any questions for the subcommittee. And
15 if not, I guess I'd ask Lisa to -- as chair, to seek a
16 vote on this.

17 MS. SOTTO: Let's turn to questions first,
18 and then we'll move forward with the formalities.

19 Joanne?

20 MS. McNABB: Just checking. In both your
21 first and second recommendations, where you talk about
22 the Social Security Administration's employee

1 verification system, is that employee or employer?

2 MR. CAPRIO: That's a drafting error.

3 MS. McNABB: Okay.

4 MR. CAPRIO: It's employer.

5 MS. McNABB: I figured --

6 MR. CAPRIO: And we're going to -- we're
7 going to --

8 MS. McNABB: Yeah.

9 MR. CAPRIO: -- check that whole --

10 MS. McNABB: Yeah.

11 MR. CAPRIO: -- acronym out, just to make
12 sure it's correct.

13 MS. McNABB: And I just want to say, even --
14 this is not a comment on this recommendation, but that
15 -- to -- for the record, there are -- there are,
16 indeed, other significant privacy concerns with E-
17 Verify, and particularly with fraud against citizens,
18 who are likely to be more victimized, because the
19 authentication procedure in E-Verify for relying on
20 immigration data is going to be more effective than the
21 authentication of employees, based on the SSA data.
22 And so, it -- the fraud would be likely to move that

1 way in the identity theft world, which we hear a lot
2 about in California.

3 MS. SOTTO: Thank you very much, Joanne.

4 Reed?

5 MR. FREEMAN: Thank you.

6 On number six, the sixth recommendation, I
7 wonder, John, if you think it would be worthwhile to
8 add, at the end, that, when considering the use of
9 commercial information sources, it should be done so,
10 consistent with applicable principles from our paper on
11 the use of commercial data that we've already
12 published. It was for a different purpose, but certain
13 fundamental principles in that, I would think, would be
14 useful.

15 MR. CAPRIO: Well, I -- that's very sensible,
16 and we did a lot of work on that, and that makes sense,
17 and that's, you know, a little extra dimension and
18 boundary to the recommendation, so I'd -- any objection
19 from anyone if we insert language to that effect?

20 [No response.]

21 MS. SOTTO: All right, so we'll -- that --
22 we'll take that as a formal amendment to the paper.

1 And, Ken, you'll help us with the procedure as to how
2 to get that done.

3 We have a few more questions. Lance Hoffman?

4 MR. LANCE HOFFMAN: First of all, I applaud
5 the product of the subcommittee. I think it was a good
6 piece of work, and very much needed.

7 It did raise a question, which I have,
8 really, for -- maybe one of the Privacy Office staff
9 can answer. You know, the PIA process is supposed to
10 identify and highlight problems before they become --
11 before there are radio commercials airing on NPR urging
12 employers to enroll in the system, especially if there
13 are potentially serious privacy issues. Does the DHS
14 PIA process look beyond privacy into the -- in essence,
15 the issue you -- the report talks about at the very
16 end, the funding -- are there -- is there adequate
17 funding to do things right, or does it not look at that
18 at all?

19 MS. SOTTO: I would ask one of the members of
20 the Privacy Office to respond. No, not prepared to do
21 so? Okay.

22 [Laughter.]

1 MS. SOTTO: John?

2 MR. KROPF: Good afternoon, or good morning.
3 The quick response -- John Kropf, and I'm the Deputy
4 Chief Privacy Officer. If I understand, your question
5 is, Does the PIA get into the funding issue? And no,
6 it does not. So, that's the simple, short answer.

7 MS. SOTTO: Do you --

8 MR. LANCE HOFFMAN: Could -- hold on. I'm
9 not going to put you on the spot further, but it seems
10 to me this might be an appropriate time to mention, at
11 least, that in the -- perhaps in the future efforts of
12 the Privacy Office, or maybe the future administration
13 would like to consider, the ongoing issue we've had for
14 a number of years of having programs go galloping along
15 with certain key privacy issues not addressed until
16 they have to be reined in, and at great expense, and,
17 you know, retooled. But, I won't ask you to make any
18 further comment, unless you want to.

19 MR. KROPF: My comment would simply be that
20 we have an approach that we, at the Privacy Office,
21 have been spending a lot of time and effort building a
22 strong network throughout the Department, and that

1 network is intended to get us involved at creation, or
2 as early as possibly at creation, so people don't wake
3 up at the end of a grand plan and think that they have
4 to add something, like privacy, at the end. We want to
5 be there at the beginning, because that's the key for
6 success, is to build privacy in by design.

7 Other questions?

8 MR. CAPRIO: Well, allow -- just a comment,
9 too, of looking at the final rule on E-Verify, which
10 was, I think, published in August, and there was a
11 comment -- it's a several [inaudible] of the final rule
12 incorporates questions raised by commenters on a
13 response. It says, "Several commenters suggested that
14 E-Verify has ongoing system security problems that
15 jeopardize the privacy and security individuals'
16 personal information. These comments focused on
17 general concerns with DHS, and, more generally, the
18 U.S. Government, and general concerns about the cyber
19 attacks." And then, the response was, "The counsels
20 disagree with these comments." And then, they
21 basically comment -- they seem to take the cyber attack
22 in the sense of attacking, like a distributed denial-

1 of-service attack or some kind of large-scale attack,
2 they didn't specifically address a range of cyber
3 security issues associated with the application. So,
4 it seemed to me -- and I didn't look at the comments,
5 and they don't include them in this rule, but it would
6 seem to me that probably some of these issues were
7 raised, but they were not, you know, considered by the
8 -- or were -- there was a disagreement by the
9 Department.

10 MR. KROPF: If I could, I had one
11 afterthought to Lance's question. There is an indirect
12 impact that a PIA can have on funding. And I'm going
13 to look over my shoulder as I give this answer, to
14 Toby. But, if a PIA is not done, it's often required
15 as part of the Certification and Accreditation process,
16 the C&A process. That's part of a C&A package. If you
17 don't have the PIA included, that may impact the
18 funding for the project. So, you could jeopardize your
19 funding without doing a PIA. Again, our challenge is
20 to make sure that that happens as early as possible in
21 the process.

22 MS. SOTTO: Any further questions before we

1 move forward?

2 Renard? I'm sorry.

3 MR. FRANCOIS: That's all right. Thank you.

4 My question relates to the third
5 recommendation. And if I understand it correctly, I
6 see the need for it, and I think that it's an excellent
7 recommendation. The way I see it is, it seems to
8 suggest that, for every person that is using, or every
9 entity that's using the E-Verify system, that there
10 needs to be, for lack of a better term, an authorized
11 user who is identifiable and authenticated. And my
12 question is just wondering whether we have had any
13 feedback from DHS or industry as to, kind of, the
14 timeframe, the cost, and maybe the practicality of
15 implementing a system, a governance system, that may be
16 very large and significant.

17 MR. SABO: That raises a -- that gets to a
18 couple of things, and I'm sure the other subcommittee
19 members -- there may be other views about this.

20 We took the position that we're not -- the
21 committee -- the subcommittee -- and clearly, the
22 larger body here -- were not technical consultants on

1 scoping a project and evaluating the cost and the
2 return on investment and doing all the things that are
3 required of Federal agencies. I mean, that -- that's
4 their responsibility, or, if they use consultants or
5 contractors to do it, that's what they do. So, we
6 didn't get into the scoping of this. We are looking at
7 the issue as an advisory -- proposing that we look at
8 it as an advisory committee, to say we see serious
9 issues, and there are a number of reasonable paths to
10 take to achieve that.

11 I would say that there are a number of -- our
12 other recommendation, that you look at the different,
13 in effect, markets for using this system -- there are a
14 number of programs in the government where there are
15 very strong, you know, approaches to identity
16 registration authentication access controls. For
17 example, the FIPS-201, which has Personal Identity
18 Verification cards being issued to all Federal
19 employees, contractors, and subcontractors, there's a
20 whole FIPS written just for it by NIST. So, there's --
21 there are a lot of initiatives where they could look to
22 the cost and the scaling of this kind of registration

1 program, but we didn't get into that, and we certainly
2 -- since this is our recommendation, we were pulling
3 information from the BPR team. We certainly weren't,
4 you know, trying to scope it out or look at the cost.
5 But, again, that's part of the -- that's part of the
6 responsibility of CIS to do that. So, I'm not -- I'm
7 not skirting you, here. There are costs, and I think
8 we alluded to that when we referenced the OMB guidance,
9 that you can't simply say, "Well, the costs are too
10 high, so we'll eliminate security and -- or reduce
11 security because it's easier to use." That just
12 doesn't cut it.

13 I think another comment I'd make is, turn to
14 the Social Security Administration to look at their
15 experience and the costs they have in registering
16 employers and authenticating and providing access to
17 individuals who come into the system, because they've
18 been doing this for a number of years.

19 MS. SOTTO: Thank you very much, John.

20 I want to -- before we vote, I'd like to
21 thank John very, very much, on behalf of the committee,
22 for taking the lead on this paper and working very

1 closely with the chair and with me and Neville
2 Pattinson for contributing also to the paper and the
3 thought process. The hope is that this will spur to
4 action those who are looking at this process closely.
5 And certainly, we're available to continue the dialogue
6 as we go forward.

7 Ken, the process with the amendment, can we
8 vote on it now and add the amendment later?

9 MR. HUNT: Oh, I think you can vote on the
10 whole thing right now. Just --

11 MS. SOTTO: Okay.

12 MR. HUNT: -- create a record that you've
13 done it. And then, it's perfectly fine for John, on
14 behalf of the committee, to, you know, take "draft" off
15 the paper and make the few other changes that you
16 talked about and submit it with a transmittal memo.
17 I'll talk about that offline, but certainly the -- as
18 long as the paper that comes in reflects the views of
19 the committee as a whole, as discussed today, we can
20 take care of that in the next -- in the next couple of
21 days.

22 MS. SOTTO: Okay, thank you, Ken.

1 I'd like to, then, ask for a formal vote of
2 the committee to adopt the E-Verify paper that you all
3 have in front of you, with the amendment that Reed
4 Freeman suggested. All in favor?

5 [A chorus of ayes.]

6 MR. DAVID HOFFMAN: Can I -- I just -- I
7 would think -- shouldn't we vote on what -- the exact
8 wording of the amendment, so that we're voting on the
9 exact finalized document?

10 MS. SOTTO: Do you have proposed wording,
11 John?

12 MR. CAPRIO: Let me try to repeat what I
13 think is -- was proposed. So, in item six,
14 recommendation six, a new final sentence, which would say
15 -- and you -- somebody can help me complete it. Reed
16 is not here. "When considering use of commercial
17 information sources," comma -- and that's where it all
18 runs out. No, I'm joking.

19 [Laughter.]

20 MR. CAPRIO: -- "the committee recommends
21 that the approaches be consistent with the DPIAC's
22 earlier guidance on use of commercial data."

1 MS. McNABB: What I wrote down was "any use
2 of -- any such use of commercial data should be
3 consistent with" --

4 MR. CAPRIO: Okay.

5 MS. McNABB: -- "dah, dah, dah, dah, dah,
6 dah."

7 MR. CAPRIO: "Any such use of commercial data
8 shall be consistent with the DPIAC's previous guidance
9 on the use of commercial data."

10 MR. DAVID HOFFMAN: So, John, can you do that
11 again, and slower, so that I could write it down?
12 Thanks.

13 MR. SABO: I'll try. But, Joanne, help me.
14 "When considering the use of commercial --

15 MS. McNABB: No, I -- just -- what I was
16 suggesting is --

17 MS. McNABB: Yeah.

18 MR. SABO: -- just start with "Any such" --

19 MR. SABO: Oh.

20 MS. McNABB: -- "use of commercial data" --

21 MR. SABO: Oh. Sorry. Go ahead. You can --

22 MS. McNABB: -- "should/shall/must," whatever

1 the right verb is there, "be consistent with," and then
2 whatever the name of that paper is.

3 MR. SABO: Well, I was saying the --

4 MS. McNABB: The principles --

5 MR. SABO: -- DPIAC's previous guidance on
6 the use of commercial --

7 MS. McNABB: Yeah.

8 MR. SABO: -- data.

9 MS. SOTTO: And I would insert the word
10 "should."

11 MR. SABO: Should.

12 DR. BARQUIN: So, then that'll be a separate
13 sentence.

14 MR. SABO: Yes. Is that okay?

15 MS. SOTTO: Okay. Now, with that -- David,
16 are you good?

17 MR. DAVID HOFFMAN: Yes.

18 MS. SOTTO: Okay. With that addition, then,
19 let's do it again. All in favor of adopting this
20 paper, with the addition that we just read, please say
21 aye.

22 [A chorus of ayes.]

1 MS. SOTTO: Any opposed?

2 [No response.]

3 MS. SOTTO: Okay. The paper will be formally
4 adopted, including the additional sentence. Thank you
5 very much.

6 Our next discussion -- I would ask you to all
7 take a sip of your coffee for so we can raise the
8 energy level around this table, because this is very
9 important -- we had discussed, at the last meeting,
10 forming a subcommittee to try to shape some issues and
11 raise to the -- to the fore some transition issues that
12 we considered to be important ones. So, we've had some
13 suggestions from folks on the committee, and we thought
14 it would be helpful to have a group discussion around
15 some issues that we view as important for the
16 transition team. So, I would ask you all to start
17 chiming in.

18 What I would also ask is somebody from the
19 Privacy Office to take copious notes, because we don't
20 get the transcript back quickly enough, and we -- this
21 is obviously an issue that requires quick turnaround.

22 We will be submitting formal written

1 recommendations based, in large part, on the discussion
2 that we have here, in the next 25 minutes or so, and
3 some of the input that we've -- that Howard and I have
4 received over the course of the last month or so, I
5 think, all of which will be covered during our
6 discussion today.

7 So, who would like to kick us off? Joanne?
8 Please.

9 MS. McNABB: I would like to restate the
10 concern I have about E-Verify, beyond the employer
11 authentication issue, which is significant, and, as a
12 transition matter, recommend looking carefully at
13 mandating E-Verify, and, before any such mandate is
14 extended, addressing the issues of employer
15 verification and then the issues of potential fraud on
16 employee verification relying on the use of the Social
17 Security database, which is fraught with problems.

18 MS. SOTTO: And this is not just a place to
19 list issues. I think it would be helpful to have some
20 discussion around issues, that if a committee member
21 raises an issue that another committee member doesn't
22 think is a top priority issue, let's hear some

1 discussion around that.

2 Richard?

3 MR. PURCELL: The development of advanced
4 technologies has overrun the ability of old law to keep
5 up, and we've seen this, globally, in the European Data
6 Directive, which is going through an evaluation
7 process. I would strongly recommend that the Privacy
8 Office at DHS participate very strongly in any
9 discussions around revisions to the Privacy Act in the
10 United States, given their extensive experience, not
11 only with PIAs and SORNs, as we've heard today, but
12 also given their breadth of knowledge they've developed
13 across areas where the Privacy Act currently exempts
14 components from developing PIAs and SORNs, for reasons
15 of national security intelligence-gathering, for law
16 enforcement, and for other purposes. It's my belief
17 that the Privacy Office that we advise here has become
18 uniquely expert in the application of Privacy Act
19 components to real-world system development, and they
20 have a unique position in advising how that act could
21 be revised to anticipate the next, perhaps, decade of
22 technology advancement.

1 MS. SOTTO: Thank you very much, Richard.

2 If you're finished with your comments, please
3 put your tents down. If you have additional comments,
4 you're welcome to keep your tents up, and we'll come
5 back to you.

6 Dan Caprio?

7 MR. CAPRIO: Thanks, Lisa.

8 One of the issues that I'd like to put on the
9 table -- and we're going to have a bit of a discussion
10 this afternoon about cyber security, which is a very
11 good start and, you know, we're most appreciative of
12 NCSD and DNI -- but, I think, as we go forward on the
13 comprehensive national cyber security strategy, known
14 as CNCI, we need to keep a very close eye both on the
15 classified and unclassified side, in terms of the
16 protection of privacy, you know, particularly of
17 information that's collected, so that we don't -- the
18 information doesn't bleed over into uses that, you
19 know, are unexpected, unanticipated, or that, you know,
20 most of the American public would probably, you know,
21 find distasteful. So, I think it's -- I'm -- you know,
22 applaud the committee and the discussion this

1 afternoon, but I -- I'd like to view it as the
2 beginning of a first step, which I hope will be a
3 collaborative process and discussion as we go forward
4 on CNCI.

5 MS. SOTTO: Dan, who would you like to see
6 involved in that discussion?

7 MR. CAPRIO: Well, I think we've -- I mean,
8 we're going to have two of the -- you know, two of the
9 players, this afternoon, Mischel Kwon and -- US-CERT --
10 and then ODNI, as the Executive Agent for CNCI. But --
11 I think it gets a little trickier on the classified
12 side, but -- you know, the other intelligence agencies
13 that are involved in CNCI. So, I think we need to
14 focus on both, and I -- both being, you know, the
15 protection of .gov and the protection of .mil. And I'd
16 like to propose, at some point, when we can, you know,
17 get the logistics right, that we participate in, you
18 know, some sort of classified briefing.

19 MS. SOTTO: Thanks very much, Dan.

20 Neville Pattinson?

21 MR. PATTINSON: Thank you, Lisa.

22 I think we've seen, over the course of the

1 last few years, several credentialing programs being
2 stood up and implemented within DHS, anything from TWIC
3 and what we see with the first responders, all sorts of
4 other credentialing programs -- REAL-ID, one of them.
5 What we don't see, I think, is consistency between how
6 the credentialing programs are put together, as far as
7 the privacy and data integrity, the security of those
8 programs, those inconsistencies between them. They are
9 clearly all done for purpose out of specific need, and
10 they're done by a team of people who are focused on
11 that role. So, you know, they've all achieved what
12 they generally have started out to do, but there's been
13 little linkage between those programs. Therefore,
14 interoperability has been sadly lacking between those
15 programs.

16 And what I think would be of very beneficial
17 use to the Privacy Office is to work with the Screening
18 and Coordination Office on interoperability goals, on
19 standards for privacy and for security and for handling
20 credentialing information on a consistent manner
21 between the programs so that we've got, then, you know,
22 a best-practice set that can offer guidance to any new

1 credentialing programs that begin within the agency,
2 within any component, that they can learn from what's
3 been done before, but have a mission of managing
4 information about identity, credentialing information,
5 in such a way that we've got consistency and,
6 ultimately, interoperability.

7 Thank you.

8 MS. SOTTO: Thank you very much, Neville.

9 Again, any comments to other commenters'
10 questions, rise your hand so that we can keep the
11 discussion on that point. And otherwise, I'll assume
12 that everybody has different points.

13 Lance Hoffman?

14 MR. LANCE HOFFMAN: Yeah, I missed the raise-
15 your-hand part, so I will get back on a comment on
16 Dan's comment.

17 I think that -- so we keep it all on one
18 topic, one at a time -- Lisa asked a question, "So, who
19 would you like to see involved?" And I want to add to
20 Dan's remarks on this, because I think it's a very
21 important issue. It hasn't gotten the attention it
22 deserves, and will deserve in the future, and we do not

1 want to be, you know -- I'll avoid the more dramatic
2 analogies, but do not want to be behind the eight ball
3 on this; we want to get ahead of it as much as we can.

4 Some people think that, because of the issues
5 related to computer systems and computer architecture,
6 "Ah, we do the best we can, but what can we do?" And
7 that's really -- we can do better than that. I think,
8 actually, the Privacy Office should be used as a -- as
9 you said, I think -- used as a leader in this, in
10 convening the appropriate people, not only for the
11 benefit of the Privacy Office and its mission, but for
12 the benefit of DHS and its mission, and also for the
13 benefit of other agencies, as well. If, indeed, we
14 have one of the -- the, arguably, best privacy office
15 around in the United States Federal Government, it is
16 its responsibility to do some outreach and bring other
17 agencies along when it -- when it's necessary. And,
18 indeed, I think DHS -- DHS being a new department,
19 sometimes that's good and sometimes it's bad. In this
20 case, it less baggage, believe it or not, than some
21 other departments that have been around for a while,
22 and can lead on this. So, I would just like to say

1 that, in addition to having the discussions you talked
2 about, the Privacy Office ought to -- also should be a
3 leader in convening other discussions with other
4 agencies. Figuring out a way to do it is part of its
5 mission, perhaps related to the data-sharing, where a
6 bunch of agencies are sharing data anyway, so you've
7 got to talk to each other, so bring this in. And I
8 think it's a much better way of starting to attack the
9 cyber security problem.

10 MS. SOTTO: Thank you, Lance.

11 Let's see, I'm looking for somebody who
12 hasn't spoken. Kirk?

13 MR. HERATH: Thank you.

14 I want to follow on, I think, sort of along
15 Lance's line of thinking. I'm going to take it a
16 little step further.

17 So, I mean, we've been doing this now for,
18 what, four years? Something like that. I mean, yesterday
19 we kicked off the initial steps of our first look into
20 how the agencies share information. And having -- you
21 know, I'm -- most of us having been involved in privacy
22 for nine, ten, more years, probably something we should

1 have done four years ago. So, I think, you know, I -- E-
2 Verify is important. I -- you know, the issues
3 themselves are important, but it all comes down to
4 program management as to whether these things actually
5 have privacy and security baked into them. And, you
6 know, the paper we just did on E-Verify -- I mean, it's
7 shocking, the lack of connectivity between the people
8 developing the policy, the policymakers, and, you know,
9 as Hugo said, the technicians. So, there is still a
10 large cultural effort that the Privacy Office needs to
11 undertake. And it's not just the Privacy Office. It
12 requires leadership all up and down the agency. And,
13 quite frankly, it probably goes all the way up to the
14 President.

15 I would like to see -- so, it's a cultural
16 educational awareness. You know, we need to stop
17 counting, you know, laptops. When laptop thefts
18 become, you know, non-events, but, you know, prosecuting
19 people or reprimanding people for misuse of data become
20 front-page news, then we know we've done something
21 right and that we have -- we don't see that yet. And
22 that takes time. I mean, that takes, you know,

1 somebody in one cube realizing that their coworker has
2 just misused their access to look up his girlfriend's
3 father, or something along those lines, so there's a
4 lot of -- there's a lot of foundational work yet to be
5 done. You know, I think we are all essentially just
6 crawling. And -- do you have a comment to make?

7 MR. PURCELL: I do, Kirk. I want to strongly
8 support the idea of the need for developing a culture
9 of privacy and security within an organization. We've
10 heard, earlier today, the good work that the Privacy
11 Office has done in --

12 MR. HERATH: Absolutely.

13 MR. PURCELL: -- establishing the SORNs and
14 the PIA processes and their leadership. This is great.
15 We also recognize that there are four Chief Privacy
16 Officers out of 23 components, and that the training
17 has been dedicated to administrative processes, like
18 PIAs and SORNs, and has not extended to the 180,000
19 individuals --

20 MR. HERATH: Right.

21 MR. PURCELL: -- all of whom, in some way or
22 other, collect, use, share, manage personal

1 information. And it's that level of affecting all the
2 individuals that I think is one of the important points
3 of stress that we might want to make.

4 MR. HERATH: Right. Yeah, I don't want to
5 downgrade -- I think -- I do think we've got the best
6 group of people in government working in privacy, so I
7 think they've done a wonderful job with what they have
8 to work with, as far as resources. And, more
9 importantly, you know, support, or lack thereof.

10 So, I do fear -- you know, I would hope that,
11 after four years of doing this, I would see more alignment
12 among all of the Federal agencies on privacy program
13 management. And somebody has to be the boss, and I
14 don't see anybody out there -- so, there's this
15 Balkanization of privacy everywhere. And I still --
16 you know, I feel like we're just sort of one -- we're
17 involved with one little aspect of it. And it's not
18 that I necessarily want to, you know, be in charge of
19 anything, but I do think sometimes that we're -- we
20 risk -- we risk losing control of the issue, and
21 somebody -- I mean, I'd rather have, you know, bad
22 alignment than no alignment, or bad leadership -- bad

1 uniform leadership -- I don't know. Because as long as
2 you get -- you know, if you get the structure in place
3 at some point, you'll get somebody there who can get it
4 done. And right now it's almost like there's a lot of
5 different groups fighting for -- fighting for space and
6 fighting for resources. And, quite frankly, I think
7 that they're taking away resources from each other.
8 So, you do have this lack of uniformity.

9 I think the convergence of privacy and
10 security -- I mean, yesterday in the IPP, you know,
11 they talked about it like, you know, it's new. I mean,
12 I think, you know, a lot of us around here have evolved
13 into more than privacy, right? So, I do -- I'm the
14 lead tech counsel, and I do information security law,
15 and -- you know, I mean, it's almost -- you can't --
16 you almost can't -- you can't draw a bright, shining
17 line between privacy and security anymore. I would
18 like to see more, kind of, partnership with security.
19 I'd like to see more security and privacy talked about,
20 sort of, in tandem.

21 MS. SOTTO: I think what we're hearing is
22 Richard's -- Richard had thrown out, in a private

1 conversation this morning, the term "data governance."

2 MR. HERATH: Absolutely.

3 MS. SOTTO: There's no question that --
4 you're right, Kirk, this is not new. I think it's
5 being named for the first time. I would -- I would put
6 in a plug for much deeper coordination among the Chief
7 Privacy Officer, the Chief Information Security
8 Officer, and the Chief Information Officer --

9 MR. HERATH: Absolutely.

10 MS. SOTTO: -- of DHS, frequent meetings --
11 frequent meetings, regular periodic meetings among the
12 privacy officers also from the various components.
13 There has to be total coordination of this sort of data
14 -- data governance --

15 MR. HERATH: Right.

16 MS. SOTTO: -- function.

17 Now, having said that, I want to also make
18 sure to, I think, put in a plug, at least personally,
19 for the independence of the Privacy Office.

20 MR. HERATH: Yes. Absolutely. No, I mean,
21 I'm not saying that one should, you know, subsume the
22 other. They have to be -- you know, everybody --

1 there's a roles-and-responsibilities matrix, I think,
2 that is lacking in the Federal Government, that most of
3 us have gone through in our own companies. Because
4 right now there's a lot of role friction -- right? -- a
5 lot of people bumping up against each other, trying to
6 do a lot of the same things. Sometimes they're doing
7 the same things in the opposite direction. And --

8 Anyway, I -- so, the program management, to
9 me, is fundamental. We can't do anything -- we can't
10 -- we can't solve any of the problems that we identify
11 as sort of philosophical problems, the grand problems,
12 you know, if the foundation is inadequate or
13 nonexistent. I mean, I do think that the paper we're
14 going to do on information sharing, the agreements, the
15 MOUs, the structure of the process -- I'm excited about
16 it, I think it's -- it is -- it has the potential of
17 taking this to the next level. And even though I was a
18 little shocked at -- that, sort of, it's as basic as it
19 is right now. I think we have an opportunity to evolve
20 it, and that's really what privacy, in my mind, is
21 about, it's just always moving the ball forward and
22 building on your processes.

1 So, the scut work of the -- you know, the
2 technical work, it's the bread and butter of privacy,
3 and it's the little things that you've got to do every
4 day, and the processes and procedures that you've got
5 to have baked into every program and process and
6 technology.

7 MS. SOTTO: Thank you very much, Kirk.

8 I just want to say a little bit more about
9 the independence of the Privacy Office. We talked
10 about it this morning with Catherine. It's so
11 critical, in my mind, that the Privacy Office remain
12 independent. While the Privacy Office certainly
13 tackles some issues that are also tackled by other
14 offices at DHS, the Privacy Office comes at those
15 issues from a different perspective, and that's a
16 perspective that shouldn't be subsumed within another
17 perspective; it must really remain an independent view.

18 I would also urge that the privacy -- the
19 Chief Privacy Officer continue to have a direct report
20 to the Secretary, and also urge the Privacy Office to
21 maintain the FOIA function, keep those functions
22 together. Where FOIA is really sort of the back end,

1 the redress, the access piece, the Privacy Act is the
2 front end. So, both have to work in coordination. So,
3 it's very important that those functions remain
4 together.

5 MR. HERATH: Yeah, and I don't -- I don't --
6 I hope nobody took my comments to say that it shouldn't.
7 I actually testified before Congress a couple of years
8 ago and said that I thought the Privacy Office at DHS
9 should be given greater independence, almost inspector-
10 general powers, and I do believe that, you know, there
11 should be, actually, a stronger linkage between the
12 component parts and the DHS; they should be a -- it
13 should be almost a hard line to the -- the component
14 parts should hardline to the Chief Privacy Officer, and
15 maybe dotted-line to their -- to their component heads,
16 so that there can be more uniformity and alignment
17 driven down through the whole organization.

18 MS. SOTTO: Thank you.

19 Ramon?

20 DR. BARQUIN: Two suggestions for the
21 transition, one which I'm sure you all expect, and one
22 which maybe you don't.

1 The one you all expect is that I believe that
2 there should be at least a Department wide, if not
3 broader, data integrity initiative. Right now, data
4 integrity, which is a fundamental, you know, pre-
5 requirement to a lot of the other issues that we've
6 been dealing with on privacy, is just nowhere.

7 The other suggestion is that I would -- I
8 would ask the new administration to consider seriously,
9 the creation of a privacy protection innovation lab.
10 What happens is that right now, you know, we get thrown
11 out all of these technologies, and then are asked to
12 try to figure out what the -- what the privacy impacts
13 are, how do we deal with it. And I believe that if we
14 took a proactive approach through an innovation lab on
15 privacy protection, we would be a step ahead, in terms
16 of creating, suggesting technologies and processes that
17 would help us go a long ways, vis-a-vis the goals that
18 we're trying to accomplish here.

19 MS. SOTTO: Lance?

20 MR. LANCE HOFFMAN: Yeah, you asked us to put
21 up our hands if we comment on an immediately preceding
22 comment, so there I go again.

1 [Laughter.]

2 MR. LANCE HOFFMAN: I am jumping up and down,
3 figuratively. I think that's a terrific idea. It's a
4 terrific idea, for a number of reasons.

5 We heard testimony -- this committee heard
6 testimony a couple of years ago, from Latanya Sweeney,
7 at Carnegie Mellon, describing her work in privacy-
8 related research that, at least at the time, was not
9 funded by DHS or a lot of other agencies, because it --
10 in essence, they didn't want to do it, for various
11 reasons. Academe. I'm from academe. The academe is
12 not structured, in general, to support or to encourage
13 these interdisciplinary efforts that are really
14 critical. There's a lot of talk about its moving
15 there, but it's moving there way too slowly for what we
16 need in the real world.

17 And we see some efforts in various funding
18 agencies -- National Science Foundation and others --
19 but they're still a drop in the bucket relative to what
20 could be done. And, indeed, DHS has its own R&D
21 component, which is, I would say, not doing a very good
22 job at all in this regard. And that's one place DHS

1 could start. But, beyond that, I think the idea of a
2 lab would be just -- would yield immeasurable benefits,
3 so I'd like to go on record as supporting that, as
4 well, and encouraging the new administration to look at
5 that.

6 MS. SOTTO: Thank you, Lance.

7 I'd like to ask that we indulge this
8 conversation for another 10 or 15 minutes. Is that all
9 right, Ken? We're supposed to break, but it -- we're
10 -- we have a lot of comments, and I'd like -- I'd like
11 to get all of them on the record.

12 John Sabo?

13 MR. SABO: I'll put the tent down. My --
14 following up on that, leading to my comment, I think
15 the lab makes a lot of sense, but it should be -- data
16 privacy, per se, is a lot -- it's analogous to data
17 security. I mean, you have -- you have procedures, you
18 have practices, you have policies, you have training,
19 and you have audits, you need controls, and so on and
20 so forth. And in the data security field, we have tons
21 of technology, tons of standards. We have standards on
22 encryption, we have standards on best practices, we

1 have risk-assessment standards, et cetera, et cetera,
2 et cetera. We don't have that in data privacy. So,
3 while I fully agree with the need for the lab, I also
4 think it needs to be accompanied by someone examining
5 the structural issues, the governance issues around
6 privacy. Privacy things we've already seen in some of
7 the DHS programs, where, you know, you're building a
8 redress system. What does "redress" mean? What about
9 individual access to records, which is required by the
10 Privacy Act, and the ability to correct errors? How do
11 you do that when you have 16 data sources that are
12 feeding a data mart or a database, and then you're
13 running an algorithm, and so on? So, I absolutely
14 agree with the need to look at individual technologies,
15 but I think what's been hugely missing is anyone
16 examining the central core components of data privacy
17 as they relate to privacy and security, how they work
18 together, beginning to build some common policies and
19 practices for the Department. And I think this fits in
20 with our recommendation, in the E-Verify, about how the
21 agencies actually talk to one another when their
22 systems are talking to one another. It's funny that

1 the privacy officers can't meet and discuss this, when
2 their systems are meeting every nanosecond to discuss
3 it.

4 [Laughter.]

5 MR. SABO: So, my specific recommendation on
6 that would be to say, let that wonderful 30-person
7 Privacy Office, which DHS has, do some things that I
8 see in other parts of DHS. I'm looking now at an e-
9 mail announcing a -- webinars being sponsored by the
10 Infrastructure Protection Directorate on such exciting
11 topics as an educational briefing for CIPAC trade
12 association members on the vision of DHS, critical
13 infrastructure protection. Do what NIST does, which is
14 -- or carry on what you've done with some of your
15 focused external facing seminars, organize some very
16 focused regular recurring thematic approaches to --
17 with state and local fusion center leaders, with
18 private sector community who are involved in DHS
19 systems and data exchange -- and begin looking at a
20 governance model, structurally, for privacy that can
21 then lead to the selection of controls, the selection
22 of technologies.

1 I mean, we have a lot of standards out there
2 to support privacy now that are emerging, but none that
3 are privacy-specific, or very few that are privacy-
4 specific. So, maybe some of the current standards can
5 be adapted to privacy, a lot of merging data governance
6 technologies and standards and so on. But, I think,
7 without a focus on this -- and, again, I --

8 One last comment. I mean, European Union now
9 has a call out for input on privacy impacts on the
10 Internet of things. And I'd say half of their staff
11 working paper was focused on RFID. The Internet of
12 things is much more than RFID, and the privacy issues
13 around it are much -- and yet, here we go back again to
14 one particular issue and one particular technology.
15 So, I'm fully in agreement with that, but I think there
16 needs to be a structural approach to this, and the
17 leadership could come out of the Privacy Office, in my
18 opinion.

19 MS. SOTTO: Ramon?

20 DR. BARQUIN: Yeah. No, I just fully agreed.
21 And when I mentioned the idea of a lab, I specifically
22 took it beyond technology, to include processes,

1 practices. No, there can be innovation in areas that
2 are not just technology, so -- 100 percent.

3 MS. SOTTO: David Hoffman?

4 MR. DAVID HOFFMAN: So, I'm hopeful, going
5 into the new transition, and I am primarily hopeful
6 because I've -- what I see is significant progress made
7 in the last couple of years. And, to me, one of the
8 things that needs to be most focused on is making sure
9 that the progress that is in flight and the things that
10 are moving, keep moving, and they don't take the ball
11 off of that. So, I group this -- the way we look at
12 this in -- I think, in private industry, that in a
13 structural way and with four different components, that
14 you need to coordinate up, down, across, and out. And
15 I see fantastic progress on all of these. And I want
16 to make sure that those continue.

17 I think the upward coordination that Mr.
18 Teufel has been able to do directly with the Secretary
19 in increasing the budget of the organization,
20 increasing the prominence of the organization within
21 the Department, has been fantastic. I think that that
22 needs to be continued. And I think there's also going

1 to be an interesting opportunity that I hope people are
2 able to make happen with coordination upward to the
3 Privacy and Civil Liberties Oversight Board. And I
4 think that's going to be absolutely critical for the
5 transition to focus on what the role there is going to
6 be there.

7 I think the coordination down has really
8 started to pick up, and this is with the component
9 CPOs. At the -- and I think this is something Kirk and
10 I have talked a lot about -- at the end of the day,
11 it's the people who really are close to the way the
12 programs are being created, and organized, and carried
13 out that can make the difference about whether
14 individuals' privacy is protected or not. It's those
15 component CPOs who are going to have a deep
16 understanding. They're the ones that if -- they're
17 trained, and if they're in there in all of the
18 components, if they're full-time government employees
19 who are at the right level of seniority reporting in to
20 the heads of the components who could really make a
21 difference, I think then coordination across, which is
22 the way this is, viewing with the other organizations

1 within the Department, like information security, can
2 be an incredible way to leverage resources and make
3 yourself more efficient.

4 And then, something that we haven't talked
5 much about, coordination out, which I think has really
6 picked up, I think could go even further and -- two
7 different categories here. The first would be outside
8 to external advisors. You have this advisory board.
9 The -- Mr. Teufel and the staff have been fantastic in
10 using us to solicit our opinions. That needs to
11 absolutely continue. I also think another form of
12 coordination out that should be increased is
13 coordination with other countries. We're going to have
14 a transition here of a new administration. A year
15 following that, our allies in Europe are going to have
16 a major transition there at the European Union. I
17 think it's a significant opportunity, and we ought to
18 prepare ourselves to take advantage of it.

19 MS. SOTTO: Thank you very much, David.

20 Actually, I'd like to elaborate on your
21 points, because the two points that I've written down
22 to make sure get covered are international and the

1 committee. So, since you've raised both, a little bit
2 of elaboration.

3 It's so critical, in my view, that we
4 coordinate internationally. There has been a serious
5 uptick, I think, in international coordination in the
6 last year or two years. There needs to be more of that.
7 And privacy really needs to be considered in
8 negotiating various policy papers with foreign
9 governments, particularly those very active DPAs in
10 Europe and in other places with active privacy offices.
11 So, I would absolutely support David's thoughts there.

12 The second is this committee. We have a real
13 brain-trust here, and I think there's been a little bit
14 of frustration, over the last couple of years, that we
15 haven't been as active as we'd like to be. We, I
16 think, as a committee, would just urge you in the
17 Privacy Office to take advantage of the expertise
18 around this table. And we come from all walks, and
19 have lots of different perspectives, and I think we
20 could add immeasurably to your work. So, I would -- I
21 would push this committee and ask that you include the
22 committee and integrate the committee in a more

1 enhanced way, going forward.

2 Tom Boyd?

3 MR. BOYD: Ana had her hand up first.

4 MS. SOTTO: Oh. Ana?

5 DR. ANTON: Thank you.

6 So, in the interest of making recommendations
7 of new possible priorities, I would like to see us be
8 more proactive than reactive. And I'm thinking
9 specifically in terms of setting the clout services
10 that the government is using, or should be using, and
11 the privacy implications of that. And I bring this up
12 as the non-lawyer in the group. So -- but, I'd like to
13 see us actually do something before it's too late.

14 MS. SOTTO: Thank you, Ana.

15 Tom?

16 MR. BOYD: Well, I -- what I wanted to add,
17 simply, was to reinforce what you just momentarily --
18 said a moment ago with respect to David's comments,
19 because I couldn't agree more with virtually everything
20 he said.

21 When we're talking about interactivity with
22 our European counterparts, it's critically important --

1 well, I think we all agree that it's critically
2 important that we -- that we do so, and that there be
3 an understanding as between the various DPAs in Europe,
4 as well as our own policymakers in this country, as to
5 what privacy means. And that includes -- in addition
6 to the regulatory regime, it seems to me that also
7 includes the enforcement culture. One cannot go
8 without the other. And there is a lack of
9 understanding, obviously, and a lack of implementation
10 of similar enforcement cultures overseas as compared to
11 the United States. And so, when we're dealing with
12 this internationally, we need to take -- look at it
13 globally, involving both the United States, as well as
14 Europe, and Asia, for that matter, in the [inaudible]
15 process and elsewhere. I think you're absolutely
16 right.

17 And I also think it's important -- and I
18 suspect we're all of the same view with respect to the
19 prominence of this office, of the -- of the Privacy
20 Office in DHS. In my sort of anecdotal exposure to
21 various departments and the Executive Branch over time
22 when it comes to privacy, this is by far the best. And

1 I think the new Secretary would be well advised to look
2 at this office as a model, frankly, for the Executive
3 Branch.

4 There is -- we talk about inconsistencies
5 within the components of this Department; you just
6 multiply that in spades with respect to the rest of the
7 Executive Branch. And this is by far, I think, the
8 best office I've come in contact with. And being able
9 to have a direct report to the Secretary is critically
10 important. I think we all appreciate that. Some of us
11 who have been in government before and had those direct
12 reports recognize that, without it, you might as well
13 not even create the office, because it'll have little
14 or no effect in a bureaucracy the size of this
15 Department. And I think -- I think Ms. -- the new
16 Secretary understands that. She's a former U.S.
17 Attorney herself, and understands big bureaucracies in
18 the Department of Justice. And so, hopefully she'll
19 recognize and appreciate the importance of that.

20 Also, if I could make another Justice
21 Department analogy, the Justice Department's Office of
22 Legal Counsel is technically the General Counsel for

1 the Executive Branch, the White House Counsel being a
2 separate and distinct entity. And it wouldn't be too
3 far from reality, it seems to me, for the Chief Privacy
4 Officer of this Department to effectively be, or at
5 least be informally recognized as being, the sort of
6 go-to model office for the rest of the Executive
7 Branch, given the multitude of responsibilities this
8 Department has and the jurisdictional lines it
9 inevitably crosses. Seems to me there are many, many
10 duplication opportunities that they could benefit from.
11 So --

12 MS. SOTTO: Yes, Richard?

13 MR. PURCELL: Following on, on that, Tom, I
14 absolutely agree, but I think that we also have to
15 recognize that the reality and the perception of this
16 office that we have spoken to today is not necessarily
17 broadly shared, particularly with key influencers. One
18 of -- you know, one of -- one of -- one of the
19 unspokens here is that there is a privacy event on the
20 Hill today to which we are not invited. And if,
21 indeed, we're correct in our assessment that this
22 privacy office is superior, we have to also admit that

1 not everyone shares that same view. And I believe that
2 one of the things that we can recommend highly is,
3 there's a lot more work to do to communicate that --
4 the superior qualities of this group more broadly.

5 MR. BOYD: I don't disagree with that at all,
6 but I -- my point in making my statement was that the
7 capacity of this office is unlike, really, any other
8 office that now exists in the Executive Branch, at
9 least with which I'm familiar, notwithstanding its
10 merits or demerits or how it's perceived in various
11 jurisdictions. The new Secretary has an opportunity to
12 begin anew and to recognize what she has to work with
13 and recognize the importance of crossing lines
14 elsewhere in the dominant departments where privacy and
15 where individual information is traded and transferred
16 and shared and the like within the intelligence
17 community and the homeland security community and the
18 law enforcement community and the like.

19 And so, all I'm suggesting is that, you're
20 right, and I recognize there are a range of different
21 views with respect to this office, and by that -- as
22 far as that concerns, this department. But, the base

1 here, which the new administration must understand and
2 the transitional -- transition team certainly should be
3 sensitized to, is what they've got to start with here
4 is a great deal better than anything I've experienced
5 personally anywhere else in the Executive Branch.

6 MR. PURCELL: And again, we agree. I just --
7 I want to warn the committee that the opportunity could
8 be squandered if we are not helpful in trying to
9 influence the perception that this is a superior group
10 of people and that they do provide good models for the
11 development and the, you know, kind of, proliferation
12 of good practices throughout the other agencies of the
13 government, as well.

14 And I just want to make sure that we don't,
15 kind of, sit on our laurels and say, "Oh, these guys
16 are great, fine," and then, three months from now, find out
17 that nobody else got that message. The message has to
18 get out in order for it to be effective. And I think,
19 frankly, it isn't. It isn't out at all. And it's part
20 of this -- the committee members, individually and as a
21 whole, part of our responsibility is to make sure it
22 does get out.

1 MS. SOTTO: Thank you very much. Those were
2 very insightful comments, Tom and Richard.

3 Joanne, I believe you have the last word.

4 MS. McNABB: Oh, good.

5 [Laughter.]

6 MS. McNABB: Two things. First, a very
7 specific thing. I would urge the new administration to
8 take another look at the REAL-ID final rule, which, in
9 spite of the best efforts of the Privacy Office and the
10 recommendations of this committee, does not adequately
11 address privacy and security.

12 Second, and more broadly, I would encourage
13 the new administration to look at the privacy framework
14 that this committee recommends, which is a risk-
15 management approach, and begin early in the
16 consideration of new programs, by address -- to address
17 the programs' effectiveness in accomplishing the
18 security goals that they set themselves, before the
19 privacy issues even come up. That's still not
20 happening consistently. And I think we put together a
21 pretty good way to look at that for DHS programs, and I
22 would encourage that the new administration look at

1 that.

2 MS. SOTTO: Thank you all very, very much for
3 a really thoughtful discussion -- really, a tremendous
4 discussion, and certainly one that was -- has been --
5 that is informed by a number of years on this
6 committee. And I think we're going to have a lot of
7 good recommendations.

8 I would ask each of you who has had such a
9 great -- such great ideas, to please send me a
10 paragraph that summarizes one or two thoughts that you
11 have.

12 I would also ask if there's any way to
13 expedite this part of the transcript, that would be
14 very helpful. Understanding that that may not be
15 possible, if you could send me that paragraph, I will
16 volunteer to coordinate putting all of these ideas
17 together into a paper. And Toby, if you were the one
18 taking notes, if you could -- we can work together to
19 get that information.

20 All right. Well, thank you very much, and
21 we'll move on to our break and reconvene at --

22 MR. HUNT: 1:00 p.m. sharp. And I do want to

1 thank the whole committee and -- for their activities
2 today, and we look forward to receiving the E-Verify
3 report and transmitting it to the Secretary and the
4 Chief Privacy Officer and the program immediately.

5 [Lunch recess at 11:50 a.m.]

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 PRIVACY AT DHS:

2 LOOKING FORWARD - ADVOCACY PERSPECTIVES

3 MR. ROTENBERG: Great. Thank you very much,
4 Lisa, members of the committee. I also wanted to thank
5 my colleagues, Jay Stanley at the ACLU and David Sobel
6 at EFF, who have allowed me to go at the beginning of
7 this time slot, because I need to go back to the Hill
8 for the hearings that they're having on these same
9 topics.

10 And I also wanted to say, actually this is
11 the first time I've had the chance to be before the
12 committee, and we're now, in some respects, kind of
13 toward the end of a process, or at least in a
14 transition.

15 And I'd like to begin, actually, by thanking
16 you, and particularly certain members of the DHS staff.
17 And I do have in mind Hugo and Toby, for their outreach
18 to the privacy community. We've had quite a lot of
19 battles over the last several years. I was putting
20 together a paper, and I found more than 50 reports,
21 cases, or campaigns that EPIC was involved with
22 concerning the Department of Homeland Security. I

1 think at one point we even made coffee mugs which said,
2 "Privacy: It's the Law" and cited section 225 of the
3 organic act. I'm happy to provide you with those mugs.

4 We were litigating, in fact, over the
5 transparency of the Department before it was even
6 created. David Sobel and I had raised some concerns
7 about the Office of Homeland Security, which, you may
8 remember, Governor Ridge helped put together as a
9 predecessor to the Department, and it outlined some of
10 the preliminary goals for the agency. And we felt that
11 some of those documents should be made available to the
12 public.

13 But, I will say, throughout the entire
14 process, I mean, we really do appreciate the efforts
15 that have been made by the Chief Privacy Officer within
16 Homeland Security, and his staff, to reach out to the
17 privacy community. I felt, sometimes, as if I was on
18 Hugo's speed dial. I don't know if, in fact, that is
19 the case. But, there has been a lot of communication.
20 And we also appreciate the fact that there have been a
21 number of important public workshops on very
22 interesting and timely topics -- the use of video

1 surveillance in public spaces, for example, RFID
2 technologies; that's very important and certainly worth
3 pursuing -- as well as recommendations that I know that
4 this committee has made on some thorny problems, such
5 as the use of contactless RFID for human
6 identification, which is an area that we have
7 particular concern about. It is actually one of
8 several areas, which I'll talk a bit more about in a
9 moment, where we think some of the security solutions
10 are actually creating new security risks. And the use
11 of contactless RFID is actually a pretty good example
12 of that.

13 All this having been said, and very much in
14 support of the efforts of the -- of this committee and
15 the work that you do in support of privacy and public
16 oversight, I have to say to you, after a little bit
17 more than five years now of watching the growth and
18 development of the Department of Homeland Security, I
19 am very, very concerned about the direction that this
20 agency is taking, and that its impact will be on the
21 privacy and civil liberties, particularly of America
22 citizens. I think we have created an agency with

1 authority and technological capability that is enormous
2 and is not well understood, even by people with the
3 best of intentions in the effort and the attempt to get
4 a better handle of what DHS has become.

5 And I say this, as I said, having spent quite
6 a bit of time over the last five years looking at
7 everything from the Automated Targeting System, to
8 passenger profiling, to RFID to border security, to watch
9 lists, to Secure Flight. On almost any of these topics,
10 I would suggest to you, if you do a Google search,
11 there's a very good chance that a page that's been
12 produced by my organization, EPIC, will come up near
13 the top of the search results you get. I can't begin
14 to summarize the amount of time, the number of reports
15 we've done, some under the heading "Spotlight on
16 Surveillance." You may know Melissa Ngo. She wrote
17 several excellent reports.

18 But, the overall picture is, frankly, quite
19 scary; and it's quite scary, because it reminds me
20 that, with the best of intentions, it is possible
21 within government to create institutions and
22 authorities that can have very dire consequences.

1 Let me give you an example of what I'm
2 thinking about when I make this point. You're all
3 familiar with the backscatter X-ray technique. I like
4 this photograph, right? This is the cover of Reason
5 magazine. So, here's a very interesting technology
6 that makes it possible to observe airline passengers as
7 if they're undressed, right? I mean, that's the
8 purpose, because we've decided that magnetometers,
9 which detect the presence of metal, do not detect the
10 presence of other devices that may pose a risk to
11 aviation security. So, we've developed some new
12 techniques that make it possible to see these objects
13 on the human body.

14 Now, there's a privacy problem here. No
15 doubt about it. The question is, How do we understand
16 it and how do we deal with it? DHS privacy staff
17 thought about this quite a lot. There was a lot of
18 discussion. And they said, "Well, obviously it's
19 inappropriate for the operators of these devices to be
20 able to observe the passenger as they're going through
21 the device; it would be as if you had X-ray vision and
22 you could see people undressed. So, a number of steps

1 were taken to address that particular concern.

2 You can display the body image as if it's a
3 chalk line, you can remove the operator from the point
4 of visual contact with the subject, and now you no
5 longer have the risk, people believed, that the air-
6 travel passenger's privacy had been violated.

7 If you stopped the discussion at that point,
8 you have barely scratched the surface of the privacy
9 impact of this technique, because, of course, what
10 backscatter is, essentially, is a digital camera that
11 captures and records an image that can be stored and
12 displayed and duplicated, and then any number of other
13 things you might choose to do with a digital image.
14 And if you go to the vendor's Web site, as I did when I
15 was researching this particular issue, you will read,
16 in fact, that the vendor was quite proud that these
17 images could be displayed on any PC-compatible monitor.
18 Right? And I said the privacy issue that the TSA is
19 dealing with, that the Department of Homeland Security
20 is trying to understand, is not the observation that an
21 individual operator will have at a moment in time of a
22 particular person, it is the collection of very

1 sensitive personal information and its possible use
2 downstream.

3 Now, of course, once we raised this issue,
4 you know, people began to listen, you know, the vendors
5 agreed to change the setting. Very interesting, right?
6 Because we're basically now just talking about a
7 toggle. Change the setting so the images weren't
8 recorded. We actually pressed for legislation. We
9 said, if there was any reason to believe that these
10 images were being recorded, not only did we want people
11 fired, we wanted the contractors off any DHS projects.
12 That's how strongly we felt about this.

13 I'm spending some time on this example
14 because I believe that, across the agency, there are
15 dozens upon dozens of instances where programs have
16 gone forward, for good purpose, keep materials off
17 planes that might pose a risk to aviation security, a
18 privacy assessment has been done, because people are
19 concerned about privacy, and the outcome is wholly
20 inadequate. Wholly inadequate. I think you would
21 reach the same conclusion if you looked closely,
22 closely, at an assessment of data mining across the

1 Federal Government. This is an enormous challenge,
2 because we have the situation today that this
3 information is being collected in unregulated fashion.

4 Now, this goes to my next key point. The
5 data-collection practices of the Department of Homeland
6 Security are not well understood. They're not well
7 understood, because the Department of Homeland Security
8 operates in a way that's very different from a
9 traditional law enforcement agency. We've spent quite
10 a lot of time, as you know, over the last several
11 years, debating, for example, the President's
12 surveillance authority, whether or not there should be
13 individualized suspicion before we wiretap a person.
14 Right? These are good, sort of, classic Fourth
15 Amendment questions, constitutional authority. Very
16 bright legal scholars of differing views -- you know,
17 there's not a single conclusion -- will reach different
18 outcomes.

19 These data collection systems, where there is
20 no particularized suspicion, where, for example, you
21 have closed-circuit television all across the Nation's
22 capital capturing images of people who live in the

1 District, people who work in the District, people who
2 are suspected of no crime, by the way. That
3 information is being collected and used with very
4 little assessment of the privacy consequences. And
5 those systems, as well, continue to grow, and, I would
6 argue, without meaningful oversight.

7 One of the key problems in understanding the
8 privacy impact of the agency's activities, in my
9 opinion, is that there are no meaningful metrics. We
10 don't have a way to gather data on a regular basis and
11 compare it over time and try to assess, Are the threats
12 increasing? Are our responses increasing? Are these
13 programs working, or are these programs not working?

14 By way of example -- a contrast -- if you
15 look at Federal wiretap law, there's a remarkably clear
16 set of factors that the government is required to
17 collect when it engages in electronic surveillance.
18 There are questions about, What was the authority? What
19 was the outcome? What was the cost? What was the
20 duration? Very interesting question in the Federal
21 wiretap law; What percentage of the information that
22 you've collected is relevant to the purpose that you

1 undertook the electronic surveillance, right? I mean,
2 it's not a bad question to be asking. If you're going
3 to give someone electronic surveillance authority, you
4 might ask the question, you know, Is it five percent of
5 what you listen to? Is that relevant? Or was it 50
6 percent? And then that data, which is required under
7 Federal law to be collected, can be compared over time
8 from year to year over region -- How does the Northeast
9 compare with the Southwest? Are some techniques more
10 effective or less effective? We have some common data
11 to look at and to assess.

12 I don't see that in Homeland Security. What
13 I see is an annual report that we struggle to get out
14 of the agency on privacy issues. And I say "we
15 struggle," among the many campaigns that EPIC has done
16 over the years -- and you may be familiar with this one
17 -- we actually figured out, when we found the statutory
18 requirement for the publication of the annual report,
19 and that it was several months late, we began a
20 campaign called "Privacy Report Held Hostage: Day 17,
21 Day 18." I mean, we really wanted that report
22 released. Now, it's half in jest, to try to get people

1 interested in an otherwise arcane issue, but the other
2 half is actually quite serious, because how else do
3 people outside of the agency assess the impact of these
4 programs?

5 Now, with full respect to this committee,
6 because I know they're a very distinguished, expert
7 people here who have spent a lot of their time, without
8 compensation, looking at these issues, and we do
9 appreciate it, I have to say, at the same time, that in
10 most areas where privacy oversight mechanisms have been
11 established, one of the key techniques of oversight, in
12 addition to the expertise of the Advisory Committee, is
13 the publication of routine reports, so that people who
14 are outside the agency who have an interest, so that
15 journalists who cover the agency who have an interest,
16 have the ability to draw their own conclusions about
17 how well the agency is addressing privacy concerns.

18 The wiretap report that I just described for
19 you a moment ago, that is a statutory requirement in
20 addition to the work that Federal judges do in
21 reviewing wiretap warrants. We have judges in place
22 who make decisions in this country about electronic

1 surveillance. And we also publish public reports, to
2 that anybody who's interested about these issues will
3 have the opportunity to draw their own conclusions. I
4 think that's critical.

5 On another front, I am also very concerned
6 about the impact that this agency has had on the
7 privacy laws of other countries. And I raise this
8 issue specifically. It was one of the issues that we
9 became aware of, post-9/11, when President Bush wrote,
10 in October of that year, to the President of the
11 European Council, and he said in his letter, which is
12 public and we've made it available on our Web site,
13 there are certain European privacy laws that cause
14 concern to the United States, as they may operate as
15 obstacles to our ability to investigate and prevent
16 future acts of terrorism.

17 Now, let me be clear on this point, there is
18 no dispute about the need to investigate and prevents
19 future acts of terrorism. That's not what I'm arguing
20 about. What we're arguing about are the techniques or
21 the legal means by which those investigations are
22 pursued. And the specific problem with what the U.S.

1 has done over the last seven years with many of its closest
2 allies, requiring them to provide ten fingerprints when
3 they enter the United States -- I don't know if you
4 have relatives who live outside the United States. I
5 do. They don't want to come to this country, they
6 don't want to see -- well, they do want to see their
7 grandchildren, but they don't want to be asked to
8 provide their fingerprints at the border, because they
9 associate with this with how criminals are treated.

10 This is part of the consequence of the U.S.
11 effort to extend new surveillance techniques.
12 Passengers from Europe coming to the United States are
13 now required to provide travel itinerary information to
14 Homeland Security, right? Who they're traveling with,
15 where they're staying. No dispute about the need to
16 prevent future 9/11s, but is such detailed information
17 required, and does it need to be kept for so long? And
18 if the United States pursues these practices, why
19 wouldn't our allies imitate them? In fact, that's what
20 they've done; they now demand fingerprints, they now
21 require passenger manifests. And what we are seeing is
22 a gradual erosion, around the world, of privacy

1 safeguards.

2 Just by way of example, the Olympics in
3 Beijing this past year, an extraordinary event, also
4 featured some of the most advanced surveillance
5 technology the world has ever seen, through the use of
6 identity cards, through the use of face recognition and
7 CCTV, which we're about to have introduced in the
8 United States. Beijing 2008 actually became a testbed
9 for surveillance practices that we are likely to adopt
10 here in the U.S. How should we feel about that, seven
11 years after 9/11, that we are innovating in the areas
12 of citizen surveillance, helping the Chinese government
13 strengthen their control, and then bringing those
14 techniques to bear on our own citizens?

15 I could go on. As I said, we've spent quite
16 a lot of time over the last several years. And I
17 apologize if my words sound a little harsh. I
18 genuinely appreciate the work of this committee, and I
19 think people that have worked with me over the years
20 know that we have a genuine commitment to the
21 protection of privacy and the rights of Americans. And
22 that is the basis of our concern.

1 But, as I look ahead and as I think about the
2 future of the Department of Homeland Security and the
3 recommendations that we will make to the transition
4 team, they'll be quite forceful. We would begin, for
5 example, by shutting down the fusion centers.

6 Let me tell you something about those state
7 fusion centers -- right? -- which began with a good
8 purpose. Almost all of these programs begin with a
9 good purpose: preventing future acts of terrorism. No
10 one is going to argue with that. Can you, as the
11 expert panel today, conclude that the fusion centers
12 have helped prevent future acts of terrorism? Do you
13 know, in fact, what they're doing? General law
14 enforcement, general public warning, general data
15 collection.

16 Let me tell you about something very
17 interesting we uncovered through our Freedom of
18 Information Act litigation. We were interested to
19 learn that the State of Virginia, which has, like most
20 states in the U.S., good privacy laws and good open-
21 government laws that protect the rights of their
22 citizens and provide some accountability for government

1 activity, was pushing to amend both its privacy law and
2 its open-government law with respect to the Virginia
3 State Police creation of the federally funded fusion
4 center. They basically said they wanted, in their
5 State, open government, and they wanted privacy
6 protection, except for the fusion center. And I
7 thought, well, that's kind of odd. I mean, those laws
8 have been there for a long time, they're fairly well
9 thought out, most criminal matters are addressed with
10 exemptions. It's not the case, generally speaking,
11 that an open-government law is going to create a
12 problem for law enforcement, intelligence gathering.
13 Those are well understood issues. But, here was the
14 State of Virginia engaged in, kind of, a wholesale
15 rollback of its accountability laws.

16 I mean, as we did some digging through open-
17 government litigation, we basically found that Homeland
18 Security and the FBI had entered into an MOU with
19 Virginia and with other states to accommodate the
20 fusion centers and to make changes in the state privacy
21 laws and the state open-government laws so the Federal
22 activities would not be subject to these state

1 safeguards. That's a very serious thing.

2 It may sound kind of legalistic, but what it
3 means is that, in addition to whatever "Big Brother"
4 concerns you might have, or not have possibly, about
5 the fusion centers, in addition to the technological
6 capability, one of the other consequences is that the
7 states are now bringing down their privacy laws and
8 their open-government laws to accommodate this
9 federally funded program. That should stop. I mean,
10 it's somewhat unbelievable, in fact.

11 We went back to the White House guidance on
12 the Federal fusion centers, and there was a very good
13 statement from this administration in the guidance that
14 it was important to properly respect our system of
15 federalism and the rights established by the states.
16 But, what happens, in practice? A lot of that gets
17 pushed aside.

18 So, we would stop the Federal fusion centers.
19 And we would probably urge that many of the new
20 technologies for border control be much more closely
21 examined. We talked, you know, at the outset about the
22 risk of contactless RFID. People are looking at the

1 U.S. -- technology experts -- I mean, people around
2 this table maybe won't say anything now, but, I mean,
3 they're just scratching their heads. Why is the U.S.
4 creating identity documents that has the practical
5 effect of making it easier to identify people at a
6 distance without their knowledge or consent? I'm not
7 an expert in computer security; I work with some very
8 smart people who are. One of the things I learned was
9 a concept called basic access control. One of the
10 first rules of identity management is that you have the
11 person responsible for the identity document in control
12 of its disclosure. Right? Otherwise, you essentially
13 open the door to all forms of fraud and theft. I mean,
14 if I can't control what information that verifies me is
15 being released to others, how do we reasonably know the
16 representations about me are, in fact, me?

17 Now, I understand we can try to construct
18 some elaborate systems to solve that problem, but talk
19 about swimming against the tide. And here we are,
20 actually funding these programs, putting them in place,
21 that make American citizens, when they travel, when
22 they cross borders, when they work for the Federal

1 Government, more vulnerable to identity theft, more
2 vulnerable to fraud. These are things, also, that
3 should simply stop.

4 So, I guess what I'm saying to you today is
5 that, as you think about the activities of the
6 agencies, and as you're making recommendations, don't
7 be reluctant to put programs into two different
8 buckets. If there are things that you think are
9 working and the privacy issues have been adequately
10 addressed, and you're comfortable standing behind them
11 and defending them, tell the next administration, "That
12 works. We have assessed it, serves an important
13 purpose, keep it going." But, if there are other
14 things that you conclude really haven't worked, with
15 serious privacy problems that have not been solved, put
16 it in the second category. End it. Stop it. I mean,
17 the taxpayers will be happy, apart from all the privacy
18 and civil liberties issues.

19 I should probably stop here. I'll take a few
20 minutes, if you have any questions.

21 MS. SOTTO: Marc, thank you so much for your
22 incredibly thoughtful and very well-informed comments.

1 We really appreciate your insights.

2 I have a couple of questions, but I'll turn
3 to my colleagues first.

4 John Sabo?

5 MR. SABO: Just a quick comment. I mean, our
6 -- we proposed, or issued, some comments a couple of
7 years about privacy framework. And one of the -- one
8 of the key issues in there was efficacy. In other
9 words, if you establish a program, and it has privacy
10 implications, you really need to begin demonstrating
11 the value you're getting out of it. And I think you
12 were touch -- clearly touching on that point. I mean,
13 are we putting into place systems that cost a lot of
14 money, have privacy invasion potential or reality, and
15 then don't deliver results? So, the question is, How
16 do we go about getting the efficacy data, the result
17 data? And frankly, that isn't usually built into
18 privacy considerations in PIAs and that type of thing.
19 You're looking at things very abstractly. So, you --
20 on the other hand, you and your FOIA requests, et
21 cetera, seek that kind of information. So, do you see
22 any way to pull those together, from a, you know, sort

1 of a privacy management perspective; that is, getting
2 the results integrated into the -- into the
3 recertification of a program?

4 MR. ROTENBERG: Well, I think -- and thank
5 you for the question -- I think part of the answer is
6 really that you need a series of firewalls. I mean,
7 you need lots of different types of evaluation coming
8 from different directions. Some of it's internal to
9 the agency. I mean, you mentioned Privacy Impact
10 Assessments; they're important. I mean, the meetings
11 with experts are important. But, you know, one of the
12 things I've done over the years, I've spent a lot of
13 time trying to understand how this United -- how this
14 country has created oversight mechanisms for electronic
15 surveillance. And the truth is, I think, by and large,
16 we've done a very, very good job. I mean, things have
17 changed over the last few years, but the main point I
18 made to the 9/11 Commission, you know, is that privacy
19 laws have evolved in the U.S. over a long period of
20 time and against a lot of obstacles. And one of the
21 keys, as I said, is lots and lots of different types of
22 oversight, you know, from lots of different places.

1 Because if there's a problem, you know, there should be
2 opportunities for people to find it. I don't know if I
3 exactly answered your question, but that's -- okay.

4 MR. SABO: Thanks. I think -- I think, as a
5 practical matter, though, it doesn't, and I'm not sure
6 we have the answer. We see a PIA process, and we look
7 at programs, and we're looking at the front end, but we
8 don't necessarily see anything coming out of the back
9 end to say, as you said earlier, This is the
10 consequence" --

11 MR. ROTENBERG: Right.

12 MR. SABO: -- "these are the number of
13 interventions we've" --

14 MR. ROTENBERG: Well, that --

15 MR. SABO: -- "had," et cetera.

16 MR. ROTENBERG: -- should concern you. How
17 do you make the evaluation? I mean, this is kind of my
18 point. And just to give one example -- I mean, and
19 this is some time ago, although this example will be, I
20 know, familiar to some people on the panel. So, in the
21 early 1990s, we had a debate with the FBI over whether
22 or not wiretap law should mandate an intercept

1 capability. Right? This was the so-called "digital
2 telephony bill." And the FBI was saying, at that time,
3 "The technologies are advancing rapidly, and we need to
4 build in techniques, so that if we have lawful
5 authority, we can execute the warrant." And, I mean,
6 again, we tried to be respectful of the opposing
7 positions, and we understood their concern, but we also
8 asked the question, "Is there some documentary evidence
9 to support this?" And we did FOIA requests. And, in
10 fact, the field offices said this wasn't a problem.

11 Now, there may have been other reasons to do
12 with it, but there wasn't the data to support the
13 policy result. And whatever your opinions might be on
14 that particular issue, I think it would concern you --
15 right? -- if you reached a judgment that way.

16 MS. SOTTO: Ramon?

17 DR. BARQUIN: Marc, you had a comment that I
18 thought was very, very important, and that's related to
19 the metrics issue, or lack thereof. And I was just
20 wondering whether you could elaborate a bit more, or
21 maybe provide some suggestions, to the Department, the
22 Privacy Office, vis-a-vis what they should be --

1 MR. ROTENBERG: Right.

2 DR. BARQUIN: -- measuring.

3 MR. ROTENBERG: Well, this is one of the
4 issues, actually, that we've -- you know, we're trying
5 to raise with the transition team and others, how to
6 get a handle on the problem. I mean, I would begin
7 with, you know, something simple. You want to publish
8 an annual report on a timely basis, and you want that
9 annual report to include numbers. Okay? The numbers
10 might include, for example, a simplified description
11 of budget authority by program area. Now, that data
12 can be found if you go digging deep into the Federal
13 budget, but it's hard to extract. And one of the
14 things that we try to do through our "Spotlight on
15 Surveillance" series was really get a handle, you know,
16 what's happening with the expenditures for E-Verify or
17 for fusion centers or, you know, for the various
18 passenger screening programs. Let's at least make it
19 easy for the public to understand how much is being
20 spent.

21 Now, let's consider another matter. One of
22 the questions that's frequently asked, and it was --

1 this was oftentimes asked of Kip Holly at the border
2 control hearings -- you know, how many terrorists have
3 you stopped? I mean, how many -- how many people cross
4 U.S. borders each year and -- last I recall, I think
5 the number was actually zero, although there are a
6 number of people who -- with outstanding criminal
7 warrants, probably several hundred, who have been
8 stopped as a result of enhanced border security. But,
9 let's get those numbers out there, too. Let's get some
10 numbers on how many people we were able to arrest at
11 the border because of our new border control systems.

12 Let's get some numbers on the number of
13 public complaints -- here's a good one -- to the TSA
14 from passengers who believe they were wrongly pulled
15 aside or wrongly put on the watch list. Right? That's
16 an interesting question. There's a lot of anecdotal
17 discussion. Any number of hearings. I'd like to know,
18 over time, is that number going up, is it going down?

19 Some of this will necessarily be subjective,
20 but I do believe, if we're going to assess the impact
21 of this agency, we need to begin to put in place the
22 metrics that let people who have differing views -- and

1 we all have differing views about how to resolve these
2 issues -- to at least begin by looking at some common
3 data, and trying to agree, you know, What is working?
4 What is not? You know, where are the harmful impacts,
5 what can we change? That's a start.

6 MS. SOTTO: I love the idea of metrics. And
7 I'm thinking about -- we do -- as John said, we see the
8 front end, we don't ever approach the back end, and I'm
9 thinking that maybe this is a project that we can take
10 on to figure out how help to systematize the process of
11 getting metrics after a program has been up and
12 running.

13 I would ask you, Marc, if you could name two
14 projects for us to take on next year, what you might
15 suggest to us. We have a -- we're in an interesting
16 position, because we don't actually get a bird's eye view
17 of the Department as a whole, we see pieces of a much
18 bigger puzzle. So, we sometimes can identify issues
19 that we think are worthy of our attention, but I would
20 say, most often we can't, and we are asked to approach
21 -- to deal with issues by the Privacy Office, where
22 they think there's an issue that needs to be managed.

1 So, from a -- from an objective and bird's eye view
2 perspective that you have, can you -- can you help us
3 with topics to tackle next year?

4 MR. ROTENBERG: I mean, that's a -- you know,
5 that's a great question. I can, you know, think of a
6 half a dozen. I mean, you know, what is personally
7 identifiable information, you know, minimization
8 techniques -- I mean, a lot of these topics, I think,
9 will be familiar to people here.

10 But, I will say, comparing the work of this
11 committee with some of the other privacy expert groups
12 that I'm familiar with -- and I'm thinking now of the
13 Article 29 Working Group or the International Working
14 Group on Privacy Protection and so forth -- I think one
15 of the things that needs to change is, I think you need
16 to be able to make more specific recommendations. And
17 I have in mind, actually -- and I had something to do
18 with the creation of this committee, but you -- and
19 John knows this, I think -- but, back in 1987,
20 legislation went through Congress, called the Computer
21 Security Act, and there was a provision in the Computer
22 Security Act that created, in a sense, a privacy expert

1 committee with 12 members, and it was chaired by Willis
2 Ware through the -- through the early years. And it
3 was actually an interesting time. It was a difficult --
4 I mean, there were a lot of debates, for example, about
5 crypto policy and a lot of very strong opinions. I
6 mean, this may seem, for people who are involved with
7 these issues post-9/11, to be, you know, a serious
8 time, but I would say it was also pretty serious in
9 those days, too.

10 And one of the things that amazed me about
11 this particular committee -- and I think it also spoke
12 to Willis's expertise -- was his willingness to try to
13 reach constructive recommendations that could be
14 implemented.

15 So, in addition to topics that you look at, I
16 think you need to think about those recommendations
17 that are -- would actually change agency practice, some
18 way that you could look back and say, you know, these
19 were the five things we wanted to see Homeland Security
20 do, and, you know, maybe they only did three, but, wow,
21 they did three things that they might not have other
22 done if the committee hadn't put forward

1 recommendations. Willis did this very well. And when
2 I was trying to think about privacy oversight
3 mechanisms, that was one I kept coming back to. So --

4 Well, thank you all, and it was nice to see
5 you.

6 MS. SOTTO: Thank you very much, Marc.

7 Okay. Could I ask -- let's see -- Jay
8 Stanley and David Sobel, please. And gentlemen, I'm
9 going to introduce both of you, and then we can -- we
10 can begin. Thank you very much for joining us.

11 David Sobel is Senior Counsel of Electronic
12 -- of the Electronic Frontiers Foundation. He directs
13 the FOIA Litigation for Accountable Government Project.
14 And David also served as Co-Counsel in the Challenge to
15 Government Secrecy Concerning Post-9/11 Detentions, and
16 participated in the submission of civil liberties
17 amicus brief in the first-ever proceeding of the
18 Foreign Intelligence Surveillance Court of Review.

19 David's handled numerous cases seeking the
20 disclosure of government documents on privacy policy,
21 including electronic surveillance and encryption, and
22 he's co-editor of the 2002 and 2004 editions of

1 "Litigation Under the Federal Open-Government Laws."

2 Jay Stanley is the Public Education Director
3 of the Technology and Liberty Program of the ACLU. And
4 he's the author, co-author, and editor of numerous ACLU
5 reports on privacy and technology issues, and has
6 appeared in numerous television, radio, and print
7 outlets across the country.

8 Prior to joining the ACLU, he was an analyst
9 at Forrester, the technology research firm, where Jay
10 focused on public policy issues related to the
11 Internet.

12 Welcome, David and Jay. And, David, could
13 you kick off the panel?

14 MR. SOBEL: I would be happy to, thank you,
15 Lisa. And thanks, to all of you, for having us.

16 I think I spoke at the inaugural meeting of
17 this group, so it's nice to be back. I'm not sure,
18 though, that the issues that I'm going to be talking
19 about have changed that much. I think maybe some of
20 the names of some of the programs are now different,
21 but I think a lot of the issues are the same.

22 You know, I -- with respect to transition

1 issues, it's kind of hard to really identify, you know,
2 what's likely to be addressable as an issue in the
3 transition. I think -- you know, I tend to think up
4 things not -- in this area, as not so much
5 administration-specific as if things are, you know,
6 sort of that easily changeable. I really tend to think
7 of things, in terms of bureaucracies and sort of, you
8 know, the ingrained cultures in agencies. And, you
9 know, this happens to be an agency that, I guess, has
10 already -- in its young life, has developed a culture
11 that, you know, really has some, you know, built-in
12 resistance to privacy issues, and I don't see that
13 magically changing as a result of a transition. I
14 mean, I think, you know, the issues that have, kind of,
15 been at the forefront since the agency's inception, you
16 know, remain, and I don't really foresee, you know, a
17 sea change in how all of these issues play out,
18 regardless of which administration is overseeing the
19 operations of the agency.

20 So, having said that, let me kind of, start
21 with, you know, a big concept, and then I'll talk about
22 some -- a couple of specific issues, just to, you know,

1 create some basis for discussion.

2 Those of us in the civil liberties and
3 privacy community, I think, you know, really, since the
4 immediate days after 9/11, have tried to get a focus
5 placed on the effectiveness part of the equation, when
6 we're talking about anti-terrorism initiatives or
7 proposals. You know, I mean, people -- security guys
8 can sit around in a room and come up with all of these
9 great ideas, but it seems like there's often not enough
10 emphasis on really assessing the effectiveness of
11 what's being proposed. And what we have always said
12 is, you know, a lot of the programs and initiatives
13 that create privacy problems have questionable
14 effectiveness at the outset. So, you know, why even go
15 down a certain road that's going to create a lot of
16 privacy issues if there hasn't been a demonstration of
17 effectiveness, or even an assessment of how likely the
18 program or the approach is to be effective.

19 And, you know, one of the issues that, again,
20 from -- almost from day one, has been with us is the
21 whole question of data mining, and the obvious privacy
22 problems that are created by the acquisition of massive

1 amounts of information, and then the data-mining
2 techniques that are applied to that. And I don't know
3 if the committee has had an opportunity -- I don't know
4 if you've had a -- had a meeting prior to this one
5 since it came out, but, you know, I would point your
6 direction -- and I'm sure you're familiar with it and
7 have addressed it in some -- to some extent -- the
8 recent National Academy's report, "Protecting
9 Individual Privacy in the Struggle Against Terrorism,"
10 and what it -- the conclusions it came to with respect
11 to data mining. I'll just read a little bit, from the
12 executive summary, which I think is very significant.

13 First, it talks about how -- the concept of
14 data mining has been successfully used in the area of
15 credit card fraud and consumer fraud detection and
16 prevention, generally. But then, the committee goes on
17 to say, "But, such highly automated tools and
18 techniques cannot be easily applied to the much more
19 difficult problem of detecting and pre-empting a
20 terrorist attack, and success in doing so may not be
21 possible at all." So, you know, this raises the
22 question of the extent to which, within the Department

1 of Homeland Security, assessments of effectiveness have
2 been made with respect to the various techniques that
3 raise concerns about privacy issues.

4 And on that point, there was a recent op-ed
5 -- I guess this is -- you'd call this an op-ed -- just
6 a little opinion piece written by James Thomson, who
7 is the President and CEO of the Rand Corporation,
8 titled "DHS AWOL: Tough Questions about Homeland
9 Security Have Gone Missing," is the title of this
10 little piece. And he, who is in a position to know
11 something about this, as well as other Federal
12 agencies, says that the Department of Homeland Security
13 isn't asking many critical policy questions. And
14 specifically with respect to this effectiveness
15 question, he says, "DHS implements most of its programs
16 with little or no evaluation of their performance.
17 When performance metrics have been implemented, they
18 have often measured inputs and outputs only, not
19 effectiveness."

20 So, I think that's an important, you know,
21 big-picture issue to look at. You know, we're talking
22 about some very invasive programs that the Department

1 puts in place that have very serious privacy
2 implications, and I'm not convinced, you know, now, seven
3 years out from 9/11, that this kind of assessment of
4 effectiveness has really even been done.

5 So, I just want to throw that out there as
6 something to look at, you know, in the context of a
7 transition or whatever. I mean, to the extent that,
8 you know, there's going to be a fresh look taken at
9 some of what's going on in the Department, I would
10 emphasize the need for looking at the effectiveness of
11 some of these programs.

12 Okay. So, now with respect to some specific
13 issues. EFF has been very involved, in the last
14 months, and very concerned about the issue of the
15 searches and -- searches and, we believe, seizures, of
16 electronic devices -- laptops, PDAs, other things -- at
17 the border, by Customs and Border Protection. We've
18 been engaged in Freedom of Information litigation in
19 the Federal Court in the Northern District of
20 California, trying to get some answers with respect to
21 the policies and procedures. And, unfortunately, just
22 last week, the Court in the Northern District upheld

1 CBP's decision to withhold, for the most part, all of
2 that policy and procedure information concerning laptop
3 searches.

4 I don't -- again, I don't know the extent to
5 which this committee has had an opportunity to look
6 into the issue, but, Lisa -- assuming that you're going
7 to ask me the same question --

8 MS. SOTTO: We have not looked at --

9 MR. SOBEL: Okay.

10 MS. SOTTO: -- this issue. But, it is an
11 issue that some members of the committee have raised
12 concern about, and specifically mentioned this issue,
13 in connection with recommendations to the transition
14 team, as issues that need to be at the top of the
15 agenda.

16 MR. SOBEL: Great. Because I -- yeah, I was
17 going to say, I'm presupposing that you were going to
18 ask me the same question you asked Marc, in terms of
19 recommendations for things to specifically look at, and
20 this would certainly be on my list.

21 I don't think I have to tell all of you how
22 significant the kinds of -- and personal and

1 potentially invasive the kinds of information contained
2 on a laptop or another electronic storage device could
3 be, but let me just throw out very basic statistic and
4 fact to put this in some context.

5 You know, people at the agency, at Customs
6 and Border Protection, will say, "Well, for years we've
7 been able to look through papers and books that
8 somebody's, you know, coming across with," so they
9 analogize it to that. Well, there isn't a reasonable
10 analogy to any amount of paper. A new MacBook Pro,
11 which comes with a 320 gig hard drive, can hold the
12 equivalent of three floors of an academic research
13 library worth of paper. Or, to put it in another -- in
14 another way, to sort of visualize, it's been estimated
15 that just one gig of electronic data would be the
16 equivalent of a pickup truck filled with paper,
17 crossing the border. So, I mean, it's really, you
18 know, not -- it's nowhere near the equivalent of the
19 old-fashioned, you know, looking through a -- quickly
20 -- a stack of paper. I mean, what the government is
21 able to acquire and store and retain under rules that
22 are not entirely clear when you're talking about

1 electronic media, is just an entirely different animal
2 than what we've seen with respect to these kinds of
3 searches in the past.

4 So, again, I don't think there has yet been
5 the amount of transparency with respect to this
6 practice that there needs to be. I will note, in
7 talking about reporting issues, that the Privacy
8 Office's recent annual report noted that border search
9 issues generally form the highest -- account for the
10 highest number of complaints that have been submitted
11 to the Department, in terms of privacy issues that the
12 Privacy Office has jurisdiction over. There is no
13 breakdown with respect to how many of those complaints
14 involve searches of laptops and other electronic
15 devices, but I think that certainly is something to
16 look into.

17 I would also say that the courts do not
18 appear to be a venue that is likely to provide a
19 meaningful solution in this area. A couple of Federal
20 appeals courts have looked at the issue -- most
21 recently, the Ninth Circuit, in the Arnold case -- and
22 the courts have concluded that these searches are

1 constitutionally permissible, but I -- there is
2 legislation pending -- or was pending in the last
3 Congress, and likely to be reintroduced -- that
4 addresses this issue. And I think it's clearly
5 something that this committee and the Department as a
6 whole really needs to take a look at.

7 The other issue -- and I mentioned, at the
8 outset, that some issues never seem to go away -- the
9 other issue I want to address is the whole question of
10 redress, that citizens who encounter various components
11 of the Department and have problems continue, I
12 believe, to really fall into a black hole when it comes
13 to the ability to get privacy problems and watch-list
14 problems resolved.

15 Now, part of this is a problem with respect
16 to Privacy Act practices within the Department, the
17 tendency to claim almost all of the Privacy Act
18 exemptions that are available to the agency when
19 publishing Privacy Act System of Records Notices, which
20 removes the rights to access and correct inaccurate
21 information maintained in agency databases. So, I
22 think the whole issue of Privacy Act System of Records

1 Notices needs to be -- to be revisited, with particular
2 emphasis on the degree to which meaningful redress is
3 provided.

4 I guess one bright spot in this area is that
5 TSA really is no longer in the business of making
6 assessments about individuals. As we all now
7 understand the Secure Flight Program, it really seems
8 to just be a matter of verifying an individual's
9 identity, and then checking that identity against the
10 watch lists that are maintained by the Terrorist
11 Screening Center, which is at the FBI. So, TSA, from
12 my perspective, finally got to the point where it just
13 threw up its hands, said, "We don't want to be in this
14 business," and got out of it. So, there's less of an
15 issue with respect to redress at TSA, I think; although
16 people who have problems at airports now have to deal
17 with the FBI, which is not an easy matter, but it's not
18 DHS's problem anymore.

19 But, the Automated Targeting System is a DHS
20 program. I continue to believe that, again, there is a
21 serious lack of transparency with respect to what ATS
22 does and how that system works. There's been some

1 conflicting information about that whether or not there
2 are, in fact, risk scores assigned to individuals or
3 not. EFF has done a fair amount of Freedom of
4 Information litigation with respect to ATS. And even
5 after going through that process, I still have a lot of
6 questions, in terms of what, specifically, ATS does
7 when -- and the kinds of information that it uses, and
8 the kind of rules that are applied to the data. So, I
9 think the public, again, you know, has some real
10 transparency and redress problems when it -- when it
11 comes to the Automated Targeting System.

12 But, let me -- let me stop there. I've
13 thrown out a number of things that I think remain as
14 issues, and I'll give it over to Jay, and then we'll
15 see what you'd like to ask us.

16 MS. SOTTO: Thank you very much, David.

17 We'll turn it over to Jay and have -- if you
18 don't mind holding questions until afterwards, and then
19 we can ask questions of both panelists. Thank you.

20 MR. STANLEY: Thank you very much, Lisa. And
21 thank you, to you all. We appreciate the opportunity
22 to come here and share our views on this.

1 In regards to the transition, you know, I
2 think that our top priorities with regards to DHS would
3 be, if I -- if I just had to list them, would probably
4 be data mining, the growth of the domestic intelligence
5 apparatus -- fusion centers -- watch lists, the danger
6 of an emergence of sort of a checkpoint society, and
7 national identity cards, which are closely intertwined.
8 And we're also concerned about many of the issues that
9 Marc and David have so ably discussed, from Secure
10 Flight to ATS and border security, RFIDs, airline
11 security laptops policy -- what we call policy
12 laundering, which Marc talked about, in terms of the
13 relationship between U.S. and foreign privacy and -- we
14 call it privacy laundering, because what we see is --
15 often, is the technique in which the U.S. pushes
16 foreign bodies, institutions, to adopt anti-privacy
17 policies, and then comes back and says, "Oh, well, we
18 have to comply with these international mandates," as
19 if they had nothing to do with their creation.

20 And definitely heartily endorse the idea of
21 metrics in effectiveness. It's one of our key points
22 for these post-9/11 years, that often there is a

1 silver-bullet mentality with "gee-whiz" technologies
2 that they -- and a commonsense notion that many of them
3 must work, when, in fact, they break down under real-
4 world conditions. And I think that -- I just want to
5 endorse that point, that, that is a key thing that this
6 committee can do, is to push -- is to push the
7 Department in that direction.

8 The DHS Privacy Office, which I sort of
9 interpreted as the subject that I would address, and
10 its role in particular, has done many, many positive
11 things. And we acknowledge that, and we take that for
12 granted. But, it's hard for us to look beyond the fact
13 that, in the past eight years during its existence,
14 privacy, overall, in the United States has really taken
15 a dive. And we are living in a time where we are
16 seeing a burgeoning security complex, security
17 establishment, grow in the United States. And privacy
18 is just getting rolled.

19 With regards to DHS, in particular, I mean,
20 there are many things, like the National Security --
21 you know, the NSA spying and so forth. And just to
22 throw a few things out with regard to DHS watch lists,

1 the need for meaningful redress, outstanding questions
2 about the REAL ID Act and its implementation, DHS's
3 FOIA backlog, and the need to address a lot of the
4 issues that we've already talked about. We've been
5 engaged in a process of trying to do some systematic
6 thinking about what the privacy oversight institutions
7 need to look like in the United States. And we're
8 currently engaged in a process of thinking about this
9 and interviewing a lot of people. And so, let me just
10 share some of our views of the future of the DHS
11 Privacy Office.

12 Regardless of how a privacy institution is
13 constructed, it seems like there's, like, six key
14 attributes that any kind of institution like that has
15 to have. And top of the list is independence. It's an
16 absolutely crucial attribute of any sort of system of
17 checks and balances, including privacy officers. And
18 it's obvious that you can't provide oversight over an
19 institution that you're not dependent -- that you're
20 not independent from, that has power over you. And the
21 actual and perceived effectiveness depend heavily in
22 independence.

1 Number two, access to information. You need
2 the ability to compel the production of information
3 from often unwilling bureaucracies and individuals, or
4 you can't do your job.

5 Number three, public disclosure is an
6 important function.

7 Number four, the power to order compliance.
8 A true enforcement body needs to have enough teeth to
9 force bureaucracies and other institutions to actually
10 comply with the law if they're not.

11 Number five, a broad mandate, a specific
12 legal provision that authorizes the body to comment on
13 legislative provisions, government, private-sector
14 plans, and so forth, that have far-reaching privacy
15 implications.

16 And number six -- and this is often -- this
17 is very, very crucial -- sufficient resources. Talking
18 to different privacy commissioners around the world, we
19 hear of a lot of them that have very broad powers, they
20 have the powers to investigate, they have the powers to
21 be an ombudsman, and so forth -- but they don't have
22 the resources to actually do it, often because the

1 function of ombudsman in which they are specifically
2 required to respond to complaints ends up sucking up
3 all their resources.

4 So, we would like to see the Privacy Office
5 at DHS move as far as possible towards assuming these
6 powers.

7 Independence is the biggest problem that we
8 have had with the Privacy Office. It's this lack of
9 structural independence.

10 In terms of access, we were glad about the
11 provision in the 2007, 9/11 Commission Act which directs
12 the Secretary to provide -- make information available.
13 But, one question we have is, How effective has that
14 proven to be in practice? And that's something that I
15 think would be good to ask. Does the Privacy Office
16 feel like it has as much access to information within
17 the Department as it needs?

18 Compliance. It seems as though the Privacy
19 Office's power within DHS is sort of more advisory,
20 doesn't really have a mandate. It has a mandate to,
21 quote/unquote, "assure" that the, quote, "use of
22 technologies sustains and does not erode privacy

1 protections," but it's not clear to me what powers it
2 has to do that within the Department. And its mandate
3 does seem fairly broad, from the language that I just
4 quoted. But, you know, it could probably be even
5 broader.

6 And in terms of resources, you know, if this
7 FOIA backlog is any indication, then it seems as though
8 the Privacy Office does not have enough.

9 We also, in our, sort of, attempts to, sort
10 of, analyze the situation, listed critical functions
11 that we think that any sort of privacy oversight and
12 institution must fill.

13 Number one is, sort of, proactive auditing
14 and oversight. Ideally, the Privacy Office won't sit
15 around, waiting for complaints to come to it, but will
16 actually be out there making sure that -- you know,
17 prevent -- trying to prevent and detect and ferret out
18 trouble.

19 Investigation. When problems or scandals do
20 arise, you need to be able to really conduct an
21 investigation outside of the -- seemingly outside of
22 the DHS context. For example, we really needed an

1 institution that was in a position to carry out an
2 independent investigation of the NSA spying scandal,
3 and we -- there was no such body.

4 DHS Privacy Office has done some
5 investigations, and we were pleased to see those, and
6 that was helpful.

7 Proactive policy leadership is another
8 critical function. You know, we're living in a world
9 where the landscape -- the technology landscape, the
10 privacy landscape -- is rapidly, rapidly changing, as
11 we all know. There are new possibilities for spying
12 and surveillance that are opening up because of new
13 technologies. And one function that the Privacy
14 Commission needs to fulfill is to provide, sort of,
15 broad public leadership and guidance to the public for
16 how we, as a society, can protect our privacy and
17 liberties in these contexts.

18 Counsel, review, and consultation. When
19 security agencies or other government bodies are
20 considering new policies or programs, it's good to have
21 privacy interests at the table on the inside, people
22 who could vet those kinds of ideas in the earliest

1 stages and steer the people away from bad ideas and
2 generally serve as sort of an institutional
3 representation for privacy values.

4 I hope that the -- you know, this kind of
5 thing is not likely to be visible to the outside, and I
6 hope that the DHS Privacy Office has done that. And I
7 think that, that's a -- you know, something that you
8 should follow and be aware of.

9 Complaint resolution, the ombudsman function,
10 is the fifth of our critical functions. And the
11 advantage on this, of course, is that it creates checks
12 on power that are accessible to anyone. And, on the
13 other hand, it can -- it's important that an agency
14 actually have enough resources to fulfill that
15 function, and that it doesn't suck up all the oxygen.
16 If the -- if watch-list redress is any indication, then
17 the Privacy Office does not have the resources needed
18 to do a proper job in this -- in this area.

19 So, we'd like to see the DHS Privacy Office,
20 ideally, do all these things. On the other hand, we
21 recognize that it does lack fundamental independence
22 and probably cannot possibly do all of them. This does

1 not mean we lack respect for the office. We believe it
2 does have a very important role to fill as part of --
3 especially if -- you know, we want the Privacy Office
4 to be improved, but we also want to see it situated
5 within a larger context, a larger sort of ecology of
6 overlapping privacy institutions that, together, fill
7 the role -- the full role of a real privacy oversight.
8 And so, I just wanted to share with you some of our
9 recommendations on that front, the context that we
10 think that the DHS Privacy Office needs to be part of.

11 And we have, sort of, four recommendations.

12 Number one, we would like to see a full-
13 fledged data-protection institution created in the
14 U.S., in the U.S. Government. Privacy is a value and a
15 right that's crucial to America and our democracy, and
16 it needs to have an institutional embodiment in the
17 U.S. Government. A concrete expression with the muscle
18 and -- to give privacy the weight that it deserves.

19 After, you know, talking to different people
20 and looking -- the Europeans have privacy commissioners
21 of various types. The U.S. Government, with its --
22 with its tripartite system, is -- does not exactly fit

1 the -- you know, the parliamentary system that the
2 Europeans have. And after looking at various options,
3 what we are thinking would probably be best would be a
4 commission structure, independent Federal agency. And,
5 in fact, the Privacy and Civil Liberties Oversight
6 Board, which recently was converted from a toothless
7 White House organ into a commission structure, although
8 it hasn't actually existed yet as that because of the
9 failure to fill its rolls, that has the potential to be
10 turned into a real full-fledged privacy body. And
11 that's what we think -- we're thinking might be the
12 best route, because it's an already existing
13 institution, at least on paper, it already has powers,
14 and -- although we think that those powers need to be
15 expanded to make -- to turn it into a real -- a really
16 effective privacy enforcement body for the government.
17 It needs to have its mandate broadened beyond covering
18 just those government programs which have to do
19 preventing terrorism, which is its current mandate,
20 doesn't have anything to do with war on drugs or simply
21 domestic -- you know, health and human services,
22 healthcare issues, are beyond its scope, that they

1 should be brought within its scope, the authority to
2 order remedies, and, crucially, of course, as I
3 mentioned, resources. If it's just going to have a few
4 -- 20-something staffers to oversee this enormous
5 security establishment with -- the intelligence
6 budget's \$57 billion, DHS budget is, what, \$47 billion --
7 then it -- no, it would just become a joke.

8 Our second recommendation is to expand the
9 authority of the FTC in the privacy arena to cover the
10 private sector, as a complement to the government body,
11 and basically expand its authority from enforcing fair
12 trade to enforcing the full fair information principles
13 in the commercial sector.

14 Our third recommendation is to create a
15 statutory White House position of Privacy Counselor
16 within OMB, akin to the position that Peter Swire
17 held, late in the Clinton years.

18 And number four is to bolster and expand the
19 powers of existing agency privacy offices, such as the
20 DHS Privacy Office.

21 And, as I said, independence is crucial, but
22 it's not everything. Privacy officers who are -- who

1 are insiders, who are part of the team, can play a key
2 role in the privacy formation process, we recognize, by
3 having a seat at the table, where they can provide
4 feedback and suggestions, shoot down really dumb ideas,
5 and so forth. And there's probably a tradeoff between
6 the independence of an organization and having a seat
7 at the table. If an insider official who goes on TV to
8 blast away, with all six cylinders, a stupid policy
9 being considered by an agency is going to probably
10 quickly lose -- quickly be shut out within the agency,
11 lose the trust of their -- of the others who work
12 within that agency. There does have to be somebody who
13 can go on television with all guns blazing, in fact
14 necessary. But, an insider, we recognize, can do a lot
15 of good, even without complete independence. And we
16 want to make sure that the Privacy Office is
17 statutorily strengthened as much as possible, and
18 institutionally strengthened, to make it independent
19 and guarantee it a seat at the table in internal
20 deliberations and policymaking. And some provisions,
21 such as the requirement for Privacy Impact Assessments,
22 probably already facilitate that.

1 And we'd like to see institutions set up that
2 encourage DHS privacy staff to have professional,
3 personal, and reputational ties to a broader privacy
4 community, and perhaps some sort of government privacy
5 office of counsel, as has been discussed, could do
6 that.

7 But, as long as the DHS Privacy Officer
8 reports to the DHS Secretary, he or she will always
9 inevitably be more of an insider than outsider, and
10 will be carried along for the ride when the political
11 leadership really decides to push anti-privacy
12 initiatives. But, as an insider, they can also play a
13 very valuable role, in the -- but, the bottom line is
14 that, in the absence of a counterpart, truly
15 independent authority, the DHS Privacy Office will
16 remain an unsatisfying, incomplete entity that's
17 chronically unable to deliver the privacy that
18 Americans deserve. It will be one hand clapping. It
19 will be -- it will be -- I was trying to think of an
20 analogy -- it will be like a cellist trying to play a
21 Beethoven trio, when the cello -- when the violinist
22 and the pianist didn't show up. You know, the --

1 they're gamely trying to play the piece, and we're
2 being asked to critique their performance, but what we
3 really need is the full ensemble.

4 So, that's sort of our big-picture view of
5 privacy oversight and, sort of, our vision of the
6 future of the DHS Privacy Office, and where we hope
7 things go from here. I hope that's useful to you.

8 MS. SOTTO: Incredibly useful, thank you very
9 much, Jay.

10 I very much appreciate the -- these are
11 incredible big-picture suggestions. They're very big,
12 but they are concrete, and that's very helpful. Are
13 you making these same suggestions, or is Barry making
14 these same suggestions, over at Bennie Thompson's
15 meeting this afternoon?

16 MR. STANLEY: I don't believe that's the
17 subject that he's addressing. Actually --

18 MS. SOTTO: Okay

19 MR. STANLEY: -- he's been taken ill, so my
20 colleague, Tim Sparapani, is filling in for him on --

21 MS. SOTTO: Okay.

22 MR. STANLEY: -- his part of that. But, this

1 is --

2 MS. SOTTO: Thank you.

3 MR. STANLEY: -- something that we're -- as I
4 had mentioned, it's sort of a work in progress, and we
5 expect to release a report on this in the coming weeks
6 or months.

7 MS. SOTTO: And I assume this is a report
8 that is meant to inform the transition committee?

9 MR. STANLEY: Yes. Oh, and I should mention,
10 in that respect, that we also have a broader transition
11 paper which covers all of the issues the ACLU care
12 about, which go far beyond DHS, but included in there
13 are some recommendations that are pertinent. It's a --
14 like, a 100-page very, very detailed document in which
15 we outline -- I believe it's 60 items that we are
16 calling on President-elect Obama to carry out when he's
17 in office, and some of those are pertinent to DHS. And
18 that's online at aclu.org/transition, and you --

19 MS. SOTTO: We will be anxious to review
20 that, good.

21 MR. STANLEY: -- can take a look.

22 MS. SOTTO: Thank you very much.

1 All right. Are you up for questions? Okay.

2 Joanne.

3 MS. McNABB: As a some-time cellist, I
4 appreciate the analogy. We don't need these -- all
5 those other people, we do just fine on our own.

6 [Laughter.]

7 MS. McNABB: Although it's fun to play with
8 them.

9 I'm -- I certainly agree with both of your
10 comments about the need for DHS and others in the
11 security world to consider efficacy of programs first.
12 And I wonder if you have -- are familiar with the
13 framework that this committee developed several years
14 ago that recommends that approach. And if you are
15 familiar with it, do you have comments on it? If you
16 aren't, will you look at it and make comments? It's on
17 the website.

18 MR. SOBEL: I haven't looked at it in a long
19 time, so I --

20 MS. McNABB: Because that's exactly the
21 approach --

22 MR. SOBEL: Yeah, I will look --

1 MS. McNABB: -- it recommends.

2 MR. SOBEL: -- I will look back --

3 MS. McNABB: Because if it doesn't meet the
4 threshold of effectiveness in countering the threat it
5 claims to counter, then you don't even get to the
6 privacy considerations.

7 MR. SOBEL: But, can I -- can I ask you what
8 your assessment is of how effective that recommendation
9 has been within the Department?

10 MS. McNABB: Perhaps not too. I will say
11 that a number of the programs the Department develops
12 did not originate with the Department, but came from
13 Congress, who apparently don't look at our framework.

14 [Laughter.]

15 MS. SOTTO: To their detriment.

16 Tom Boyd?

17 MR. BOYD: Thank you.

18 Jay, I wanted to ask you -- you made a number
19 of recommendations, as Lisa has observed, in -- pretty
20 grand and far-reaching -- potentially, recommendations
21 for the Privacy Office at DHS, but, really, as an -- as
22 a foundation for all of that, I think you observed that

1 independence is sort of a critical precedent for any of
2 these kinds of powers or responsibilities. How would
3 you structure an independent office of -- Privacy
4 Office here? What do you mean by "independent"?

5 MR. STANLEY: I think that -- I mean, what I
6 meant to say is that as long as the Privacy Office
7 reports to the Secretary, it's never going to be truly
8 independent, and it probably won't satisfy the
9 independence half of the equation, but it could do a
10 lot of good on the inside or advice side of the
11 equation.

12 MR. BOYD: Who would it report to, then, if
13 not --

14 MR. STANLEY: Well --

15 MR. BOYD: -- the Secretary?

16 MR. STANLEY: -- one possibility would be,
17 sort of, the inspector-general side of things, and
18 maybe it would make sense to mandate a -- that each
19 inspector general have a -- have a deputy who is
20 focused on privacy issues, who is separate from an
21 agency -- an agency chief privacy office. To be
22 honest, we're still working -- struggling with this and

1 working on it. And I -- I think that, you know, that
2 the real independent organization has to be this
3 commission, which is outside of DHS entirely, and that
4 is the best, sort of, structure that Congress has come
5 up with in a hundred -- since the ICC, or whatever, for
6 creating independence within the Federal -- within the
7 Executive Branch.

8 MR. BOYD: But, that would have jurisdiction,
9 presumably, over the entire Executive Branch.

10 MR. STANLEY: That it would have?

11 MR. BOYD: Yes.

12 MR. STANLEY: Yeah. That's what we would
13 like to see. Yeah.

14 MR. BOYD: Okay.

15 MR. STANLEY: So, I think that this is a
16 question that you should keep -- that I would -- I
17 would recommend that you keep in your minds, which is,
18 as you watch the Privacy Office and talk to them, you
19 know, what can be done to increase their independence,
20 and what makes sense, and where are the failures in
21 that area?

22 MR. BOYD: Thank you.

1 MS. SOTTO: In looking at Toby's face while
2 you were talking about some structural issues, I think
3 it would be helpful for the two of you to have a
4 discussion.

5 MR. STANLEY: I very much plan on doing so.

6 MS. SOTTO: Questions?

7 John Sabo?

8 MR. SABO: A question, I guess, to David, but
9 to, maybe, both of you. You know, the issue of redress
10 gets more complicated, or accountability, or sort of
11 finding where you can access records, and correct them
12 -- there's a whole set of issues in data privacy which
13 are complicated by the networked environment of data
14 flows that we have, or the source of data. You may
15 have multiple sources, and it's being integrated and
16 going into systems, and then decisions are made that
17 impact citizens, et cetera. So, if you think about
18 redress in that sense, as opposed to, "Well, I've had
19 an unpleasant experience at the border because my
20 laptop has been confiscated, so I'm going to file a
21 complaint" -- if you think about it in terms of data
22 correction or access to records in today's networked

1 environment, have your organizations done much thinking
2 about how that can be accommodated in an environment
3 where you may not know where the data is collected
4 from, as a citizen, or the impact on you may not have
5 been caused -- the immediate impact is because you run
6 into a particular system, but the ultimate impact on
7 you has been because there's data-quality problems with
8 data that has been obtained from two other sources.
9 So, could you talk about your views about how that can
10 be addressed, from a -- either from a policy
11 perspective or a business process?

12 MR. SOBEL: Sure. I mean, I think the reason
13 why the question possibly can't always be answered as
14 to, "What was the source of the data that created the
15 problem?" is that there really isn't any
16 accountability. And when I talk about accountability,
17 I mean a right of judicial review, that the citizen who
18 has a persistent problem that is creating such a
19 serious impediment to their ability to freely travel, or
20 gain employment, or whatever it is, that citizen who is
21 the victim of some bad data that's in some government
22 database that is resulting in their name being put on a

1 list that is creating a problem for them; they should
2 have a right to go to court and get the answers to the
3 questions that you're asking. And they don't. And, I
4 mean, I don't know if it's within the purview of this
5 committee to make a recommendation to Congress, but
6 ultimately that's where the right has to come from.

7 You know, I have always believed that, so
8 long as these redress issues remain within agencies, so
9 long -- you know, if the limit of redress is, "Well,
10 there's, you know, a committee within DHS that will
11 look into it," I don't think that's going to solve the
12 problem, and it doesn't appear to have solved the
13 problem yet. It's only when the intelligence analyst
14 who is putting someone's name on a list based on some
15 information that he or she is looking at is going to be
16 held accountable and asked to explain, "What was the
17 thought process that led you to put this person's name
18 on a list?" -- until that's the reality, that, that
19 person, in putting a name on a list, knows that, at
20 some point, they might be asked, in a court, to justify
21 that act, then I don't there is going to be the --
22 really, the audit trail, in effect, that needs to be

1 created to pinpoint what the piece of information was
2 that ultimately led to the problem.

3 MR. SABO: Just to follow up on that, I mean,
4 the example you used would be classified information
5 gets put into a -- you know, the -- it's integrated
6 into the watch-list data and then sent out to different
7 agencies. But, what about data quality? Do you think
8 we need for less -- for systems that are not relying
9 on, you know, classified information or terrorist data,
10 but things like E-Verify, where you have data --
11 database systems that naturally will have errors in
12 them, and yet -- so, data quality becomes an issue. Do
13 you think we -- there should be standards related to
14 things like data quality, that we don't have today,
15 generally? Or --

16 MR. SOBEL: Well, I think ultimately it's in
17 everyone's interest, both the citizen and the
18 Department, to be looking at, and dealing with,
19 accurate information. And when you're talking about
20 personal information, the person -- the only person
21 who's in a position to assure the accuracy is the
22 person that the information is about. So, for -- an

1 example is, if DHS gets bad P&R data from an airline,
2 and it indicates that I traveled to Saudi Arabia, when,
3 in fact, I didn't, you know, that's bad information
4 that is mucking up the analysis within the Department,
5 and we -- I would think both I and the Department would
6 have an interest in correcting that error. But, for
7 some reason, the Department has seen fit to exempt
8 these databases from the Privacy Act requirement of
9 giving access to citizens and giving them a right to
10 correct inaccurate information. So, you know, I think,
11 ultimately, you've got to give the ability to the
12 affected citizen, because they're the only one with the
13 incentive, and they're the only one with the knowledge,
14 to provide correct information that resides in these
15 databases.

16 MR. STANLEY: And I would just add -- I mean,
17 these problems that we're seeing, which are really the
18 essence of, sort of, the Kafkaesque problem, which is
19 that these giant bureaucracies, which are bigger than
20 any one person, become circular, and there's no end to
21 it. And the watch-list attempt -- you know, the watch-
22 list system in which there are nominations and so

1 forth, is the perfect example of this. I mean,
2 they're, in many ways, a consequence of overuse of
3 personal information. And this obsession with
4 information-based security, which attempts to seek
5 security by finding out as much information as you can
6 about subjects -- and I think that it's a -- it's a
7 dangerous road that we're going down, and we're going
8 down it very, very quickly and setting up these
9 institutions very, very quickly, without there being
10 time for redress mechanisms to evolve.

11 And just one last thing, which is that Jeff
12 Jonas, who many of you probably know, is -- has worked
13 on, sort of, data-tethering ideas and so forth. And
14 so, if you're not familiar with the things that he's
15 written, on a very practical level, that might be
16 something that's worth looking at.

17 MS. SOTTO: Yeah, we've heard testimony from
18 Jeff, and have spent a good deal of time with him.
19 Thank you.

20 Kirk?

21 MR. HERATH: I just have, I guess, a comment
22 and a -- and a question. One of the first things that

1 we did, four years ago, was a -- you know, looked at watch
2 lists, and redress was central to that paper -- the
3 concept of due process, I think -- I know, to me,
4 personally, is very important. I mean, to be fair, I
5 mean, has -- as a -- has the process at least gotten
6 better -- slightly better? Or, I mean, one of the
7 things that Lisa's written down for us to revisit is
8 whether or not, despite our best efforts -- and I --
9 and we do have a very narrow purview here -- you know,
10 has redress really backslid to the point where we were
11 four years ago? Because I had the impression that things
12 were slightly better.

13 MR. STANLEY: You know, I think there's a
14 problem, in terms of publicly available information.
15 As Marc indicated, you know, it would be helpful if we
16 had more specific information, in terms of numbers of
17 complaints and, you know, numbers that are resolved.
18 But, you know, barring that -- and, you know, we don't
19 see that, at least on then outside -- those of us
20 outside of the agency don't have access to that kind of
21 information. My sense is that, you know, the TRIP
22 system and the various redress mechanisms that have

1 been put in place probably are helpful with resolving
2 the easy problems, where it's just clearly a case of
3 mistaken identity, and, you know, once, you know,
4 somebody brings something to the attention of someone
5 who has the ability to resolve a very basic, easy-to-
6 identify problem, it probably gets resolved. But, you
7 know, the problem of a name that, you know, is given a
8 -- an individual who's given a bad risk assessment by
9 the Automated Targeting System based on some bad
10 information in some database, I don't think that that
11 problem has yet been resolved.

12 So, I think, yes, probably the easy -- the
13 easy problems have -- are, you know, more solvable than
14 they were four years ago. But, I think the hard ones
15 probably remain unresolved.

16 MR. HERATH: I mean, I guess I actually am --
17 do recall, just in the last couple of weeks, the --
18 reading about a woman who was -- her 18-year-old -- 18-
19 month-old son was -- had the same name as, like, a
20 Basque terrorist or something, and, despite her best
21 efforts, she couldn't get him on planes, even though it
22 was -- it was an absurd -- it was visually absurd, that

1 this 18-month-old child couldn't logically be the
2 Basque terrorist. Actually, I think she testified
3 before Congress just recently or --

4 MR. SOBEL: I mean, anecdotally, I have heard
5 about people who, you know, despite their best efforts
6 and, you know, their resorting to the redress that the
7 agency has made available to them, continue to have
8 problems when they go to the airport. But, again, I
9 don't think we've got any hard statistics on how
10 prevalent those problems are.

11 MR. STANLEY: I mean, my experience is, you
12 can go to any cocktail party and you can find somebody
13 who's on the watch list, or knows somebody in the
14 family who is. So, whether there's been marginal
15 improvement is, in some ways, an unimportant question.

16 MS. SOTTO: Richard?

17 MR. PURCELL: May I recommend that the
18 committee ask the Privacy Office to provide us some
19 statistical information about whether or not the
20 redress process is -- how it's operating, not only to
21 -- in a snapshot, but over -- in a trend analysis that
22 works, and perhaps separating out exempt versus

1 non-exempt type information and giving, perhaps, even an
2 administrative briefing, if it's necessary, just to
3 inform us? The anecdotal stuff drives me nuts. I'm
4 not sure what to do with that.

5 MS. SOTTO: Thank you, Richard, I think
6 that's a terrific suggestion.

7 Ken and Martha, I'm going to throw out some
8 ideas. How many complaints are there? How many are
9 resolved, and how quickly? Other ideas?

10 MR. PURCELL: Well, I -- it's always
11 interesting to know if the watch list is increasing or
12 decreasing in scope, and whether -- and what causes
13 those kinds of fluctuations in it. If there are
14 hundreds of thousands of people on the watch list, I
15 think that perhaps the world may be more dangerous or
16 less well informed than we think.

17 MS. SOTTO: Thank you.

18 Lance Hoffman?

19 MR. LANCE HOFFMAN: Expanding Richard's
20 suggestion beyond the watch list, as long as we're
21 building up a to-do list or to-consider list, I think
22 that should be expanded beyond the watch list. And, in

1 general, programs that are looked at by the Privacy
2 Office could have that kind of statistical question
3 built in, baked in, if you will, rather than us having
4 to come back later and say, "Oh, by the way."

5 MS. SOTTO: What I would like to suggest to
6 this group is -- I've just jotted down some notes on
7 new projects. You've been very, very helpful in giving
8 us food for thought, and one of those ideas here is a
9 project on measuring effectiveness after the fact. So,
10 I think we'll come back and think about what that
11 really looks like, what the boundaries of that project
12 ought to be. I think these are terrific suggestions.

13 Other questions?

14 [No response.]

15 MS. SOTTO: Okay. Thank you so much, David
16 and Jay. We really appreciate your presence here
17 today. Thank you.

18 MR. SOBEL: Thank you.

19 MR. STANLEY: Thank you.

20 MS. SOTTO: I would ask our next panel to
21 come forward, please: Steven Chabinsky, Mischel Kwon,
22 and Peter Sand. They're out in the hall.

1 MR. BOYD: Lisa? Lisa, with respect to your
2 earlier comment, when -- your dialogue with Richard, I
3 mean, there are inevitable -- there are innumerable
4 cases, as we all know, of people who have been, as the
5 Basque infant was, identified erroneously and cannot
6 get that corrected. So, how long it takes and what
7 kind of anticipated adjustments are intended for the
8 program, are critical, if we could get that out of the
9 -- out of --

10 MS. SOTTO: Yeah, I'm not --

11 MR. BOYD: -- the Privacy Office.

12 MS. SOTTO: -- I'm not sure Martha heard
13 that. Could you repeat that?

14 MR. BOYD: Yeah. What I said was that we all
15 know, anecdotally -- and I share Richard's frustration
16 about that -- we all know, anecdotally, of many cases
17 in which individuals, of whatever age, are inaccurately
18 identified with those on the watch list, and face
19 economic, as well as personal, disadvantage. And so,
20 how long it takes to correct that, which can take a
21 long time under current practices, as I understand it,
22 becomes critical. And so, what I'd -- what I'd

1 personally be interested in, and I think we probably
2 all would be, is not only how long does it now, what
3 kind of adjustments or reforms are anticipated to try
4 to make it a better and more responsive system?
5 Because individuals are the ones who are harmed here.

6 MS. SOTTO: And you know what would be
7 helpful? We've now tasked you with something -- if you
8 could just, maybe, shoot back a couple of lines to the
9 committee, saying that, "This is what we're going to
10 provide to you," that would be great. Thank you.

11 Tom, thank you for refining that.

12 MR. SABO: Another thought I had -- and I
13 mentioned to Dan on that -- is it may be that, in
14 answering some of the questions that are raised about
15 outcomes and effectiveness, the IG -- the IGs are
16 always doing studies -- when I was in government, we
17 didn't necessarily like them, but there are always
18 questions being asked about the -- you know, the
19 efficacy of a program or its outcomes. I mean, at any
20 given time, you probably have studies going on
21 throughout DHS. So, I -- a question for us might be to
22 inquire as to, Have there been any IG studies looking

1 at these issues, such as, you know, the search issue or
2 the data quality issues that we've talked about? And
3 I'm -- I know we've had at least one time when we had
4 an IG speak to us, but not on this kind of issue. It's
5 just a thought.

6 MS. SOTTO: I think that's a great point.

7 Since our liaison -- liaisons are out of the
8 room, could you, maybe, put that into an e-mail to them
9 and ask for a response? Thank you.

10 All right, we'll take a two minute breather
11 while everybody's gathering back, while the next panel
12 gathers.

13 [Recess.]

14 MS. SOTTO: Thank you. Thank you, to our
15 next panel, for joining us. I'd like to make the
16 introductions and then kick it off with Steven.

17 Steven Chabinsky is Deputy Director of the
18 Joint Interagency Cyber Task Force Office of the
19 Director of National Intelligence. That's a really
20 long title. In this capacity, Mr. Chabinsky assists
21 the Director of National Intelligence in fulfilling his
22 obligation to coordinate, monitor, and provide

1 recommendations to the President regarding
2 implementation of the President's Comprehensive
3 National Cyber Security Initiative.

4 Mr. Chabinsky's home agency is the FBI, where
5 he holds the position of Chief of the Cyber
6 Intelligence section responsible for leading the FBI's
7 analysis and reporting on terrorism, foreign
8 intelligence, and criminal matters having a cyber-
9 threat nexus.

10 Mischel Kwon is the Director of the U.S.
11 Computer Emergency Readiness Team in the National Cyber
12 Security Division of the Department of Homeland
13 Security.

14 Thank you for joining us, Mischel.

15 Mischel is an IT professional with more than
16 26 years of experience, and she was named the Director
17 in June of 2008. As the Director for US-CERT, Mischel
18 is responsible for the operational mission of US-CERT
19 and for analyzing and reducing cyber threats and
20 vulnerabilities in Federal networks, disseminating
21 cyber threat warning information, and coordinating
22 incident response activities.

1 And our final speaker of the day is Peter
2 Sand. And Peter is the Director of Privacy Technology
3 in the Privacy Office in the Department of Homeland
4 Security.

5 Thank you all for joining us. Steven, do you
6 want to kick off the panel?

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 CYBER SECURITY

2 MR. CHABINSKY: Yes, thank you for allowing
3 me the opportunity to present before you today. What
4 this group is doing is extremely important, and,
5 indeed, of course, what the Department of Homeland
6 Security is doing is extremely important. We have very
7 real and growing threats against our nation, and it's
8 important that we respond to the challenges that our
9 adversaries present, consistent with our Constitution
10 and with the privacy and civil liberties rights that we
11 all enjoy and hold dear.

12 In that regard, I've spent a fair amount of
13 my career, first in legal counsel in the FBI, trying to
14 make sure that, within that organization, we enforce
15 the law, consistent with the law. And I've had the
16 good fortune to work with most of the other agencies in
17 that time period of my government service, and have,
18 without exception, found a cadre of Federal employees
19 who all want to do the right thing, and who seek out
20 legal guidance and privacy and civil liberties advice
21 as best they can find it. So, there's a very willing
22 community of government employees who are looking not

1 only to fulfill their charge within the Federal
2 executive agency, but also who are looking to do that
3 quite consistent with both the spirit and, of course,
4 the actual body of the law.

5 And with that in mind, what we recognized was
6 that our adversaries, of course, have it much easier
7 than we do, so we're being attacked, on a daily basis,
8 through cyberspace. And we can discuss what the word
9 "attack" means, but, for purposes of this group and
10 this panel, why don't we focus on the protection of our
11 information and confidentiality that we've lost as a
12 nation, both as individuals, as businesses, and, in
13 fact, as government agencies. So, there are any number
14 of adversaries, be they criminal, terrorist
15 organizations, or foreign nation-states, that have
16 found the tools -- many readily available, others far
17 more sophisticated -- necessary to compromise, likely,
18 most outward-facing Internet system we have. There's
19 probably somebody somewhere that has the capability and
20 the sophistication to do that. I don't want to
21 overreact or suggest to this group that everyone has
22 access to all of our systems at all times, but I would

1 also be equally remiss if I were to suggest to you that
2 I have high confidence that any individual system has
3 not been penetrated or that there's not a persistent
4 presence of an adversary within that system. That's
5 sobering.

6 And when I say that, I think about a large
7 stream of threat and vulnerability vectors. And I'm
8 not talking entirely just about our vulnerability to
9 remote attack through the Internet, although hacking is
10 the most discussed and perhaps the most that we see,
11 perhaps because it's the most that we observe, because
12 that's where our technologies focus. But, let's, for a
13 minute, just to all be on the same page, understand
14 what these threat vectors are when we're talking about
15 a high-technology networked society, and, in fact, a
16 global networked society.

17 We start off with the actual manufacture,
18 supply chain of the products we use, and the vendors
19 and the shipment routes that they take. And each of
20 those areas has an opportunity for an adversary to
21 actually manipulate the hardware or the software so
22 that, by the time you receive a product, it's difficult

1 to know whether or not it's trusted. So, we have an
2 issue with the trusted nature of our operating systems,
3 our software, our applications, our hardware, and then
4 the network routers and devices that connect us all.

5 And then, if you push that out a little
6 further, we do have the remote-access threat that
7 everyone is aware of, that we see, that people can
8 penetrate our systems, and can do so with relatively
9 little sophistication.

10 And then we have what I would call expanded
11 access or proximity access. So, that would be the
12 ability, based on geographic location, to acquire
13 information. And a good example of this would be
14 wireless. So, if we are transmitting our signals
15 wirelessly, we can expect that somebody can capture
16 that through the air. And if it's encrypted, we can
17 worry about whether or not they can decrypt it, or,
18 better yet, whether or not they already have a
19 keystroke logger on our machine so they already have
20 the key and don't have to decrypt it. But, I'll call
21 that proximity access, that, through audio or visual or
22 wireless frequency means, people can capture our

1 information.

2 And then, last but not least is insider
3 access. So, if you have gotten the trusted nature of
4 your hardware and software, you feel that you have a
5 trusted system, you believe that you have the security
6 in place, that you have a trusted environment to
7 alleviate our concern about these proximity access
8 problems, there's an insider threat. And the insider
9 threat, I think, to be best understood, we need to step
10 back from thinking that it's the outsider who is
11 designed or determined to do us ill. Oftentimes, it's
12 one of us unwittingly being used, duped, socially
13 engineered to bring something into our system. And
14 therefore, we become the insider; of course, completely
15 unwittingly, but ever so effectively as were we witting
16 of what we were doing.

17 And so, in light of this, I'm here to say
18 that we're operating in an environment that is
19 untrusted. And how do you build trust into the
20 confidentiality of our information, trust into the
21 ability to feel that our information has integrity or
22 that we'll be able to have access to our information?

1 And then, to add to our dilemma, it's not
2 even all about information. Some of this conversation
3 affects physical systems, and we've probably all heard
4 the term SCADA or Process Control System -- SCADA,
5 Supervisory Control and Data Acquisition; PCS, Process
6 Control Systems, or simply Control Systems. These are
7 the -- for lack of a better way of phrasing it, the
8 mechanical processes that are enabled by computers.
9 And so, whether you're going to regulate the
10 temperature of a nuclear reactor or open up a dam, this
11 is not done by brute strength any longer of getting out
12 your 12 strongest employees and saying, you know, "pull
13 or push or measure." It's done through computer
14 monitoring, measuring. It's taking those instrument
15 feeds, and then it's controlling hydraulics. And so,
16 one could readily imagine, if those systems, if the
17 computers that are in control of them, fell into the
18 hands of our adversaries, what havoc would be wreaked.
19 So, we are now talking about untrusted environments,
20 where we have to protect our confidentiality,
21 integrity, and access to information, and our faith in
22 the ability to control our own Process Control Systems.

1 So, that's a daunting task.

2 And if you add to that the notion that this
3 is not a responsibility that is singularly for the
4 government or singularly for private industry, and
5 extends, as well, beyond our borders, you realized,
6 then, what we have been facing and what we've been
7 struggling with.

8 I am not heartened, or perhaps I should say
9 I'm actually disheartened, by the fact that, were we to
10 look at speeches about computer security dating back 10
11 years, if you were to look at some of the congressional
12 testimony or other speeches on the matter of where
13 we've been, you would hear words that are strikingly
14 similar to what I'm saying today. Now, that makes it
15 easy for the speechwriters, but it really doesn't
16 encourage those of us who are trying to increase the
17 security of our nation.

18 And so, we find ourselves, I would suggest,
19 in a situation where the threat, quite frankly, has
20 outpaced our ability to defend. And so, year after
21 year, the threat increases in sophistication and
22 number, and our defenses, quite frankly, do not keep

1 up.

2 So, what do we do in the face of this
3 sobering news? We've been doing a lot, and we've been
4 doing a lot for a decade. And I think many in this
5 room have been part of that, and have been part of
6 making sure that we do that consistent with the rules
7 that we hold dear. And we've recently started
8 considering whether our approach has been effective.
9 And in realizing that the Government's approach has not
10 been as effective as we would have liked -- and that is
11 not to say that we haven't made progress, but the
12 progress has not been sustained at a quick enough pace
13 -- we decided to go back to the drawing board and bring
14 together government agencies that are sitting in this
15 space to try to figure out, What can we do better? And
16 the evolution of that conversation, which started to
17 occur last year, developed into the Comprehensive
18 National Cyber Security Initiative, which you've asked
19 me to discuss today.

20 And that Comprehensive National Cyber
21 Security Initiative was the product, really, of 22
22 departments and agencies and components that got

1 together and thought through the threat vectors that I
2 described earlier, and tried to figure out where each
3 of them fit within helping our security in those areas,
4 and where we had gaps, and where we, strategically, can
5 start focusing to make a difference.

6 And what happened, I think, was instructive,
7 in that a lot of agencies came to the table and say,
8 "Well, I actually have a part of that, and I have a
9 piece of that." And prior to getting everyone
10 together, I think the natural inclination was to look
11 to the sector lead and presume that, that agency or
12 department had it covered, and almost had exclusive
13 ownership of it. And there's something, in a way, I
14 would argue, that's perhaps easy, and therefore,
15 Congress, I think, perhaps prefers it to have a single
16 bellybutton to push and to say, "Oh, that agency,
17 they're in charge of that portion." And to some
18 extent, I think we allowed ourselves to get into an
19 area where we had leads for certain issues, and those
20 departments and agencies were leading the effort, but
21 they weren't leading the community, necessarily.

22 And so, we saw more stovepiping than we would

1 have liked to. So, that was almost the balance, that
2 if you put an agency in charge of a particular
3 function, and you say, "Run with it," they will, but it
4 might not be together with other agencies that are
5 lesser players, but still players.

6 And one of the things that I think the CNCI
7 helped achieved was, not only a unity of purpose, but,
8 again, an integration of the agencies working together
9 and realizing the nature of their portfolios and how
10 they need to work together and how they impact one
11 another. And as I go through what are essentially 12
12 discrete, but integrated, portions of the CNCI, you'll
13 begin to see how they would obviously affect one
14 another. And the good news is, is that the departments
15 and agencies began to see that, as well, and we met
16 regularly to ensure that everyone's equities were being
17 protected.

18 So, let's run through them quickly, and then
19 I'll turn over for our next speakers and then make sure
20 that we are able to provide an opportunity for your
21 questions.

22 But, we started looking first at how we start

1 really kind of creating a front line of defense,
2 focused, in the first instance, on government systems.
3 And I almost want to give you the end of this story,
4 because a lot of people, when they start hearing the
5 initiatives, will immediately jump to the conclusion
6 that this has nothing to do with protecting the
7 critical infrastructure in the private sector, which
8 owns and operates 80 to 90 percent of everything we
9 need to survive, day in and day out. So, let me just
10 start by stating that no such thing happened in our
11 consideration. We very much were aware of the need to
12 work with industry and to share with industry, and how
13 much of an issue getting this right with the private
14 sector is to ensuring our national economy and national
15 security is protected.

16 So, starting off, though, we were looking at
17 government systems, and we realized that we had, in the
18 government, well over 4,000 Internet access points that
19 were outward-facing. So, one could readily imagine the
20 difficulty of ensuring that we are monitoring at an
21 effective rate, and certainly in a consistent manner,
22 with updates to patches, and the like, over 4,000

1 access points. I think of it in a different way, using
2 -- to use an analogy. In a hospital, you would not see
3 more than one entrance or exit to the nursery, because
4 there's something very valuable to protect inside that
5 room. And so, if you're going to effectively act as a
6 sentry to monitor what's going in and out of your
7 sensitive networks or your private information,
8 similarly you would not have, I think, 4,500 points that
9 you should be looking at, with all the budget
10 implications per agency that that would entail, as
11 well.

12 And so, notionally, we looked at the
13 Department of Defense, which had already engaged in
14 boiling down and condensing their networks, and we
15 believed that, in the civilian Executive Branch
16 agencies, we could get that number from 4,500 down to
17 somewhere around 100. And very effectively, almost
18 within the first six months, the number was reduced by
19 about half, to a bit over 2,000, and we're still on
20 course to be able to do that. And that actually sets
21 up the ability for initiatives that are going to
22 follow.

1 Initiative two has to do with ensuring that we
2 have better intrusion detection systems on our
3 government networks, and that we could have some
4 situational awareness to determine whether different
5 agencies are under similar attack. So, notionally, the
6 idea is to ensure that we're doing consistent
7 monitoring, with the ability, then, to look at what
8 we've discovered. It might surprise people, or perhaps
9 not, to know that there are a lot of government
10 agencies, and probably, for that matter, corporate
11 organizations, as well, that have somewhat robust
12 intrusion detection systems in place, with no ability,
13 then, to actually look at the results of the logs. So,
14 this would be similar to owning a jewelry store or
15 having a camera, finding out, the next day, that half
16 your merchandise was stolen, but having nobody to look
17 at the videotaped footage. And so, this is
18 unacceptable.

19 And so, the first step in this process is to
20 ensure that we have vital intrusion detection systems
21 in place. And that's nothing novel. And the Einstein
22 2 Program that's -- that is running this through DHS

1 has -- and I'm sure you'll hear more about it -- a
2 Privacy Impact Assessment that was made available to
3 the public a while back.

4 Initiative three is actually a step past that;
5 instead of just worrying about intrusion detection,
6 we're looking at intrusion prevention.

7 Intrusion detection is fun. Intrusion
8 detection, as someone described it -- and this will not
9 transcribe as well, because there's a visual to this --
10 it's basically looking at the attack, and seeing it
11 land, and saying, "Oh, that's going to hurt."

12 [Laughter.]

13 MR. CHABINSKY: So, nobody likes to be in
14 that game. Far better to actually be able to stop it.
15 And so, intrusion prevention, similar to firewalls that
16 you might have, exists with some ability to actually
17 deflect or figure out what you want to do when you
18 start seeing the incoming. And there's commercial off-
19 the-shelf products that do this, as well. And so,
20 again, I'm not sure that the -- that, notionally,
21 intrusion detection or intrusion prevention are
22 something that you would say raises different issues

1 than those you've already considered, but those that
2 you've already considered are substantial. So,
3 whenever you're doing any intrusion detection,
4 obviously you have to ensure that that which you're
5 looking for either directly has a -- that there's a
6 direct assurance that what you're looking for pertains
7 to the commission of a crime or some attack against
8 your systems, or that you have reason to believe that
9 the behavioral aspects of it, even if you hadn't seen
10 it before, are anomalous enough to suggest that
11 something is occurring criminally to your network.

12 I would pause just to remark that what we're
13 talking about is only intrusion detection and
14 prevention over Federal branch -- Federal Executive
15 Branch civilian systems. It doesn't reach entirely to
16 .mil systems. We're not talking about the intelligence
17 community systems, in this regard, when I talk about
18 this initiative. And for certain, we're not talking
19 about the .com space.

20 Moving past that, our initiative four has to do
21 with cataloging government research and development.
22 If we're really going to make a difference in this

1 space, we have to determine how much money the
2 government is putting into the technologies that are
3 going to help our security. And agency by agency, I
4 think there's good fidelity on what research-and-
5 development money is going into what projects. But,
6 across the government, there is actually no current
7 ability to determine how much we're spending on any
8 particular area of security for research and
9 development, nor is there, therefore, a way to
10 determine what gaps in research we have. So, this was
11 significant. And that's proceeding, as well, quite
12 well.

13 Initiative five, I think, does raise some
14 privacy issues, of course, that have been considered,
15 but initiative five is connecting our centers of
16 excellence, so it raises the old question of, How do
17 you bring together information from different agencies
18 that may have been acquired under different
19 authorities? And, for certain, the information-sharing
20 environment, which has more of a history in this area,
21 has been looking on the legal and privacy front at
22 these issues, and everyone is quite aware of the issues

1 we're facing in that regard.

2 This would be a good opportunity for me to
3 step back and explain that when we were developing this
4 CNCI, not only were the Privacy and Civil Liberties
5 Offices engaged within Department of Homeland Security,
6 and ODNI, and Department of Justice, but, of course, the
7 legal OGCs and Department of Justice were involved
8 every step of the planning of this, so there is -- this
9 behind the backdrop of a lot of planning that wasn't
10 after-the-fact, that "This is what we've decided to do,
11 now tell us it's okay." It was actually part of the
12 conception.

13 Initiative six has to do with viewing the
14 counterintelligence aspects that are peculiar to cyber,
15 and whether our national strategy for
16 counterintelligence needs to be more specific and
17 focus, really, on the cyber counterintelligence plans.

18 Initiative seven is how we are going to better
19 consider securing our closed classified networks. It
20 would not be the case that, simply because there would
21 not be a remote access likelihood, that the systems are
22 without ability to infect. As I described earlier, the

1 ability to control some of the supply chain, insider
2 access, expanded access still provides enough
3 opportunities to make it worth our focus to determine
4 whether our closed classified networks need greater
5 protection, and to specifically focus on that.

6 Initiative eight concerns education. We've
7 realized that the Federal Government workforce, as well
8 as the defense industrial base workforce, as well as
9 the American workforce at large, is not being developed
10 with the high-tech capabilities that our country once
11 prided itself in. And one would recognize immediately,
12 if you were to look at a lot of our graduate programs,
13 that even to the extent that we have schools that are
14 full of enrollment, that mostly we're graduating
15 foreign nationals who are returning to their home
16 countries. And I have nothing against that part of it,
17 except for the "mostly." So, I would like to make sure
18 that we're getting some American ingenuity and
19 scholarship in the hard sciences, and certainly that we
20 have the education and training that's needed, so that
21 we can have a competent workforce to allow ourselves to
22 have our economic and national security concerns taken

1 into consideration by our workforce.

2 Our ninth initiative, we refer to as "leap-
3 ahead." The leap-ahead initiative really is trying to
4 get out of the daily grind of looking at our
5 vulnerability and mitigation strategies to determine
6 whether technologies exist, five or ten years down the
7 road, that could actually be game-changers to change
8 the playing field, such that a lot of the
9 vulnerabilities that we're seeing now would actually
10 not exist, because the technology would have changed so
11 much that we're on a different platform.

12 At the most fundamental level, an example I
13 give of this has to do with video cassettes or tape
14 cassettes and how we used to be always concerned about
15 writing over what we had recorded. And so, we had that
16 write-protect notch. And someone certainly must have
17 spent a lot of time considering how to invent that, and
18 creating the hardware that would make sure to look for
19 that in order to record. And then all of a sudden the
20 CD and the DVD came along, and we were able to play
21 those and have storage on those, and all of a sudden
22 the write-protect feature, that would include some

1 physical nob that you would push, was completely -- not
2 superfluous, it was just the old technology. And so,
3 that concern faded. And so, now when you put your CD,
4 you're not worried that you're going to mistakenly
5 press "record" and record over that.

6 And that's, in concept, what I'm talking
7 about with leap-ahead technologies, how to develop a
8 more stable, secure network that will alleviate some of
9 these pressures that nation-states and corporations and
10 individuals are facing now.

11 Our tenth initiative has to do with notions
12 of deterrence, primarily starting out at a national
13 level. So, a lot is happening to us, and we have to
14 try to determine what are effective ways to try to
15 prevent it, from a deterrent perspective. Obviously,
16 criminal deterrence typically means long jail sentences
17 and law enforcement that can track people down and make
18 sure that they know that the cost of an intrusion would
19 be more costly than whatever they could seek to gain.
20 And we have to look at that, as well, with terrorists
21 or nation-states that are now using our networks to
22 intrude against us. How do we come up with a strategy,

1 a deterrent strategy, that would make the cost of
2 attacking us over these new technologies most costly
3 than the benefits?

4 Our eleventh initiative within the overall
5 CNCI has to do with supply-chain risk management. I
6 would stress the risk management of that. This is not
7 saying that we should have a local supply chain for all
8 products and goods; it's that we have to learn better
9 how we can identify what risks we have to our threat
10 actors -- vulnerabilities, consequences -- make sure
11 that, in evaluating that, we can mitigate the supply-
12 chain risks associated, not just with doing business on
13 a global basis, but doing business, quite frankly, in
14 untrusted environments even within our own country.
15 So, this is not an us-versus-them problem. But, that's
16 the supply-chain risk management initiative within
17 this.

18 And then, twelfth, saving the best for last,
19 I would say, then, is, How do we work between
20 government and industry to transition the knowledge
21 that we're getting from all of this and make sure that
22 we've secured the nation as a whole, and that the

1 entire focus of this campaign is not our government
2 systems.

3 So, let me stop there, because that was a --
4 kind of a lot to discuss. I would say that I'm not
5 sure if it was immodest to call this the Comprehensive
6 National Cyber Security Initiative. There are those
7 who say that it's a good start, but more needs to be
8 done. I think that that's probably true of every
9 hurdle we face. So, I will leave it to others to
10 debate whether the comprehensive nature is
11 comprehensive enough, and whether there are other
12 aspects that we need to consider and need to pursue.

13 But, I would say -- and I would certainly
14 challenge anyone to say otherwise -- that we really
15 have to do everything that's on this list. And we've
16 been working on this, now, since as early as January of
17 2008, when the President adopted the CNCI within a
18 presidential directive, which, itself, is classified
19 and, therefore, not commonly available, but it's
20 National Security Presidential Directive 54, which has
21 the -- which has the combined name of Homeland Security
22 Presidential Directive 23.

1 And so, with that, I will turn over the mike.

2 MS. SOTTO: Thank you so much, Steven, that
3 was really incredibly informative.

4 Why don't we hold questions and hear from our
5 panelists, and then we'll -- but, write down your
6 questions.

7 Mischel?

8 MS. KWON: Thank you. And thank you very
9 much for asking me here today.

10 My name is Mischel Kwon, and I am the
11 Director of US-CERT. I did take this position in June
12 of this year, and I took a little bit different
13 position than the last Director of US-CERT. We
14 restructured US-CERT, looking forward to the great deal
15 of work that we had in front of us, and it made a lot
16 of sense, and it was the only way I was going to take
17 that job.

18 So, US-CERT is now divided into three
19 separate divisions, which is the way it should be. I
20 happen to run the operations portion of US-CERT, so I'm
21 the man on the ground doing the work, and I am the
22 operator, and that's the way I like to look at US-CERT

1 operations.

2 We have two other divisions. The Federal
3 Network Security Division -- and this is the division
4 that is heading up the TIC Initiative now, and will be,
5 in the future, heading up more of the compliance work
6 to ensure that our networks are performing with best-
7 practice IE practices. We also have the Network
8 Security Deployment Division. This is the unit that is
9 deploying Einstein 1 and 2 today, and will be deploying
10 the other tools that US-CERT will need to monitor and
11 defend and reduce vulnerabilities in the Federal
12 network space that is our jurisdiction.

13 So, with that in mind, I'm going to stick
14 primarily to the operator's point of view, unless you
15 have questions on other areas that I can answer for
16 you.

17 But, looking at how US-CERT's mission has
18 changed, especially in regard to the CNCI, you look at
19 a great change in the way we operate and the size of
20 US-CERT. When I joined US-CERT, in June, we were a 34-
21 man organization, which is pretty small. And now we're
22 moving to a much more operational/technical position,

1 where we're actually going to have tools that allow us
2 insight into malactivity in the Federal civil space.
3 So, with this, we have to grow. And I did prepare some
4 talking points here, but I'm not going to follow them
5 directly, but you'll have to bear with me as I use my
6 notes to make sure that I cover all of these points.

7 So, our biggest change at US-CERT is our
8 size. So, we're going to be growing significantly,
9 more than doubling our size over the next year, and
10 then again the following year. And we are doing this
11 in, not just a technical arena, so we're not just
12 analysts sitting in seats analyzing data that goes by
13 us, but US-CERT is more than that. Once we identify
14 that something has occurred, we also have to
15 communicate and coordinate the cleanup effort of that
16 attack. So, with that, we're focusing, not only on the
17 technical, but we're focusing the people and the
18 process.

19 So, the technical part of this job is
20 actually the easy part. The hard part of this job is
21 the people-and-the-process part. And so, we're
22 focusing on the people and process part as our co-

1 division, the NSD, is focusing on deploying the
2 technology.

3 So, we are in the process of increasing our
4 staff and also mentoring and training our staff, so
5 we're developing comprehensive training programs and
6 mentoring programs for every position in US-CERT so
7 that we can eventually certify those people in those
8 positions so that we do have skilled workers that
9 understand the processes that they're supposed to
10 perform and are efficient at their work.

11 We're also looking at facilities expansion.
12 We're going for a temporary facility right now, just
13 across the hall from where we live, because as we -- as
14 we hire more people, we are running out of space on the
15 US-CERT floor. So, we're looking at deploying, this
16 year, a temporary facility, and hopefully, in the
17 coming years, a more permanent, larger home that will
18 not only house US-CERT, but have the capability of our
19 partners joining us, our agency partners.

20 So, we realize, at US-CERT, that the role of
21 US-CERT of not a domineering role, but it is a partner
22 role. And we realize that all of the departments and

1 agencies that we serve are our partners in this
2 mission. So, with that, we would like our partners to
3 be able to join us on the US-CERT floor in defending
4 those agencies. So, we will need a larger -- a larger
5 space.

6 We are expressing our capability needs, as
7 far as technology is concerned, to the NSD so that we
8 can get tools that help us track incidents, help us do
9 trending on those incidents, visualize the data that we
10 receive, and be able to identify attacks and malware
11 more quickly and efficiently on the operating floor.

12 But, our main focus today is a customer
13 service focus. We are trying to become better partners
14 with the Federal civil space; to be clear, the
15 executive branch, non-DOD agencies. We are -- we have
16 realized it's a partnership, we are reaching out to
17 these agencies, offering assistance in detecting
18 attack, as well as mitigating the attack, and we're
19 also bringing the agencies together, because a lot of
20 these agencies have good security operation centers
21 within the agencies. And we feel it very beneficial to
22 US-CERT and the other agencies for a good sharing of

1 information within the Federal civil space. So, we're
2 working on that partnership aspect and the customer
3 service aspect.

4 And in focusing on customer service, one of
5 the things that we realized that we needed to really
6 hone in on is making this a sustainable, repeatable,
7 and actionable process. Someday, I won't be the
8 Director of US-CERT, but I hope US-CERT can stand on
9 its own and the processes will follow. In order to do
10 that, I need to have these processes documented and
11 certified. So, we're moving to a Six Sigma process in
12 US-CERT to certify our processes and to ensure all of
13 our staff is trained, that they understand the
14 processes, they follow the processes, and we produce
15 good product, good, sound technical product for our
16 customers, and that we provide them with good customer
17 service. So, we are definitely focusing on the people
18 part of that aspect.

19 We are also focusing on some of our new
20 tools. A lot of you have heard about Einstein 2, and
21 we are focusing on the new deployment of Einstein 2, as
22 we still sustain our deployment, initial deployment,

1 small deployment, of Einstein 1, and we continue to
2 work through the procedures and processes for Einstein
3 2.

4 We've also created a new program, called the
5 Joint Agency Cyber Knowledge Exchange, or JACKE -- and
6 nobody give me a hard time about this; I allow my
7 analysts to name the program. But, the JACKE program
8 is an -- is a great opportunity for information-sharing
9 within the Federal agencies. It is a once-a-week
10 meeting. It is a sharing platform, where the agencies'
11 technical representatives come together and talk about
12 the current government-focused attacks.

13 It is true that we still have a few CIOs
14 attending, and we welcome them, and that's fine, but we
15 hope to eventually have more and more technical
16 representatives at the JACKE meeting. It is an
17 education process. It's a process about learning for
18 the Federal civil government to understand the
19 intrusion sets and attacks that affect Federal
20 Government systems, in particular. It's also a
21 wonderful opportunity for them to share with each
22 other, especially the security operations centers that

1 are -- that are of excellent caliber, that have
2 information to, not only share with US-CERT, but with
3 the other agencies, so that we all become astute.

4 We're more than aware that this is a
5 partnership, that everyone has to play in this ball
6 game. US-CERT's not going to be the panacea and is not
7 going to solve the security problem for the Federal
8 Government. This is a team sport, and everyone is
9 going to have to participate and play in the game. So,
10 doing this together is a lot more cost-effective and a
11 lot easier than doing it separately.

12 We're also looking at deploying customer
13 liaisons to the agencies to ensure that US-CERT is
14 providing the service that they need from us, as well
15 as the agencies providing the information US-CERT needs
16 to better detect and protect those agencies.

17 We're developing standard operating
18 procedures. For example, standard operating procedures
19 for our call center, so that when you call US-CERT, you
20 get the same consistent service every time you call.
21 So, we're definitely focused on that people part.

22 We're also definitely interested in the

1 trusted Internet connection. We talked earlier about
2 not using DoD terminology in talking about the Federal
3 Government, but I do look at it as reducing the attack
4 surface. And I -- and that's very important, because
5 we do have to control the amount of space we actually
6 have to look at in order to make this cost-effective.
7 So, we're definitely supporting the TIC Initiative,
8 and, in the TIC Initiative, deploying more Einstein 2
9 so that we can monitor those areas more closely.

10 It is important -- it is important to do
11 this, for a number of reasons. We would not build a
12 secure facility without someone watching the gate. We
13 need to be watching. And not only we need to watching
14 across the government, but each individual agency needs
15 to be watching their own gate. Again, a team sport. I
16 think that's really important to talk about.

17 It is important to understand that Einstein 2
18 -- Einstein 2 is an intrusion-detection product, and
19 that it is a passive sensor -- it runs on a tap, not in
20 line -- and that we do have a Privacy Impact Assessment
21 for Einstein 2 and Einstein 1, and Peter will talk more
22 about that as we go along.

1 Privacy is very important to US-CERT, as it
2 is important to DHS. Along with the Privacy Impact
3 Assessment, we also have minimization of procedures to
4 ensure that PII, or U.S. person's information, or any
5 other information that an analyst might come across, is
6 handled appropriately. And we also have privacy
7 training for our analysts, so that they understand how
8 to handle this data and what to do if they come across
9 it.

10 We also have processes with the systems that
11 are deployed that allow for logging and auditing of the
12 behavior of the analyst. So, that's important to
13 understand.

14 So, those are the big changes that we see in
15 US-CERT, which is a lot of change, a lot of growth,
16 moving to a more structured environment. That's taking
17 a little bit of getting used to for my staff, but it's
18 -- it's moving along, and it's progressing very well.

19 We've had some current testing of our
20 processes that have been very encouraging. And I'm
21 very excited about our partnerships with our
22 departments and agencies. I think this is a really

1 good way to implement security. We can now look at
2 security incident response as a life cycle, as a
3 feedback loop. We see a threat, and there's a
4 vulnerability. It's exploited and attacked. We
5 mitigate that vulnerability. And then we reflect. We
6 reflect and we look at what caused that vulnerability,
7 change our IE policies and procedures, fix the problem,
8 and then we can close the incident. I think it's
9 important to have that reflection piece in the civil
10 government so that we don't repeatedly see these
11 problems happening again. And I see a lot of the
12 things that we're doing today as that reflection, and I
13 think that reflection needs to continue.

14 So, I thank you, again, for having me.

15 MS. SOTTO: Thank you very much, Mischel.

16 Peter?

17 MR. SAND: Thank you very much.

18 I'm going to talk a little bit about the
19 Privacy Impact Assessment for the Einstein 2 program.
20 I believe it was included in your packet; if not, it's
21 on the back table; if not, it's on the Web.

22 We also did -- as Mischel was mentioning, we

1 did a Privacy Impact Assessment for Einstein 1, back in
2 2004. We did that PIA before that program was
3 launched. The same thing with Einstein 2; we completed
4 the Privacy Impact Assessment before the program was
5 launched. And if you look at the two documents, you
6 can also see how our Privacy Impact Assessment process
7 has changed over the four years. That's something that
8 we've talked about over the course of this day in
9 different ways. This is a nice, tangible way to see
10 how the DHS Privacy Office has matured in its analysis
11 of programs.

12 And I'm going to highlight just a few
13 different areas that are covered in the PIAs, and tie
14 them back to the Fair Information Practice Principles
15 that we use as our guiding principles, to give you a
16 sense of how some of the philosophies that we live by
17 translate into tangible privacy protections within an
18 operational program.

19 The first is data minimization specifically
20 related to personally identifiable information. The
21 idea is, you minimize your privacy issues by minimizing
22 your collection of PII. So, the less privacy-sensitive

1 information you have, the less risks there are, the
2 less concerns you have.

3 So, when you look at Einstein, and as we
4 worked through the PIA process, the first question we
5 had is, What information is Einstein 2 collecting?
6 What is the data? And then, Is there a connection
7 between the data and people?

8 And in working with the program and going
9 through the analysis, the first thing that presented
10 itself was the scope of the data itself. In other
11 words, what is Einstein 2 looking at? And it's looking
12 at traffic that crosses the threshold between a
13 particular agency and the Internet, which means two
14 things. It means the Einstein program does not look
15 inside the networks of agencies, so it's not looking at
16 internal traffic, and it's also not looking at external
17 traffic across the Internet. It's looking at a very
18 specific, narrow band of traffic. That's one way to
19 minimize data.

20 Another way is to look at the data itself.
21 And Einstein 2 brings with it the work of Einstein 1,
22 specifically focusing on flow records, which are

1 basically kind of trend-type data related to the
2 network traffic. So, you could look at how the traffic
3 itself is moving. You look for anomalous activity, the
4 anomalous patterns in the traffic itself. So, that's a
5 very, kind of, narrow slice of data. It doesn't
6 include any content. So, when you look at data
7 minimization, that's one area we focused on, to say,
8 well, you know, one thing to highlight is that this
9 particular type of use of Einstein is just looking at a
10 very narrow band of traffic -- again, within that
11 narrow scope, in terms of crossing the threshold. So,
12 that is one of the functionalities of Einstein.

13 Two is bringing forward the functionality of
14 Einstein. One, which is just looking at that -- the
15 flow-record/traffic/trend data.

16 The second is what Einstein 2 is bringing
17 with it, which is the intrusion detection system, which
18 actually looks at content. So, there, we spent a
19 little more time doing the analysis, because you're
20 looking -- you're talking about full detailed network
21 traffic. And the issues are, What kind of traffic is
22 it, and what are the concerns there?

1 And the data minimization process related to
2 the intrusion detection system, you know, the network
3 traffic, is focusing on the way that the data is pulled
4 out of the -- part of the data in that -- the general
5 flow that's of interest to Einstein. And it's only
6 data that is matched specifically to a signature of
7 malicious activity which has already been identified.
8 So, of all the traffic that's throwing -- that's
9 flowing through Einstein, the only thing that the
10 analysts are going to really look at are things which
11 they've already identified as being malicious code.
12 So, that, again, minimizes the data.

13 So, you're really only talking about -- of
14 all the data that is out there in the world, you're
15 really talking about a very specific set, and it's look
16 at for a very specific purpose, which is matching
17 things that have already been identified as bad, and
18 pulling that out and analyzing it, and doing the triage
19 and the rest of the fixing there. So, that's data
20 minimization.

21 Another principle that we live by is use
22 limitation. It's the same basic principles, but

1 instead of looking at the data itself, it's looking at
2 how that data is used. And again, the more you can
3 limit that, the less privacy exposure there is.

4 So, here the question is, What happens with
5 the data that you use, that comes out of Einstein?
6 What's actually being done with it? And here the focus
7 is on the process itself. What are the analysts
8 looking for? What interest do they have in the
9 elements that could be PII? And when they look at that
10 data, what is it that they're actually looking for, and
11 what do they do with it?

12 And again, working with the program, we
13 identified that their specific focus is on identifying
14 characteristics of events -- intrusions, attacks. So,
15 there may be situations in which an element of PII,
16 like an e-mail address, could appear in something which
17 has been pulled out of the traffic flow because it
18 matches a signature. But, their focus is on analyzing
19 that as a characteristic of the attack, it's not about
20 attribution. It's not about looking for who the people
21 are, it's about analyzing the different characteristics
22 of a particular event or attack. So, they're looking

1 at -- and here, I'm speaking on behalf of the
2 Directorate, from our perspective -- what we've found,
3 working with them, is that they're looking at -- they
4 would look at an e-mail address as just a
5 characteristic. It's about the person, it's not the
6 fact that it's a real person's e-mail address, it's the
7 fact that that was used as a characteristic of the
8 event or the attack, because they're looking at it as
9 --

10 MS. KWON: And, Pete, if I can just add, we
11 only capture 64 bytes of data. So, it's really hard to
12 even fit a full e-mail address in 64 bytes. So, we've
13 minimized the risk of even capturing anything that
14 could be construed as PII information by restricting
15 the amount of packet data that we can capture. So, the
16 minimalization procedures have really limited any
17 privacy implications.

18 MR. SAND: And then, the next thing we looked
19 at is what they -- do they do with the information once
20 they've -- they've done the analysis, then what? And
21 they basically write a report that says, "This
22 happened," and it's a pretty high-level report, in

1 general. It just says, "This happened. You should
2 know about it." And if there are any specific
3 questions about the specific traffic, they actually
4 refer the person asking to the agency who owns the
5 data. Because, like we talked about earlier, this is
6 something which is an add-on to all the existing work
7 that a particular agency is doing to defend our
8 networks and their computers, so all the traffic is
9 already going straight through to the agency, and if
10 somebody who has a question about the event wants to
11 look at the data, they can go right to the agency,
12 because the agency itself is going to have all the
13 detailed data. So, US-CERT's role, in terms of using
14 this information, is pretty focused, and that is
15 alerting people and doing the analysis and
16 understanding what the attack was, and then explaining
17 that to people.

18 So, that's use limitation.

19 Finally, notice and transparency. How do
20 people find out that this exists? The first way, and
21 the most comprehensive way, is the Privacy Impact
22 Assessment itself, which is about 20 pages long. We

1 have one for the first one [inaudible] and it really
2 explains the program and how it works. There's also an
3 arrangement with the agencies who are participating,
4 that they have to alert their people that this is going
5 on. So, the individual people who are logging onto
6 their machine have to be notified that there is this
7 kind of intrusion detection activity going on, and they
8 should be aware of it.

9 And then, there's also the external audience,
10 the people on the other side of the transaction. And
11 there, we point to the website privacy policies that
12 announce that there's also this analysis of the data.

13 And the relationship between people doing the
14 analysis and the agencies is formalized in a written
15 agreement that the agencies have to sign onto,
16 basically saying, "Yes, we agree that we're going to
17 participate, we're going to follow these protection,
18 and we're going to -- we're going to make sure that
19 we're all doing the right thing together."

20 So, those are just the highlights of the
21 protections that are identified in the PIA. And the
22 more details are in here, and we're certainly here to

1 answer any questions that follow.

2 Thank you.

3 MS. SOTTO: Thank you very much, to our
4 entire panel. And thank you, Peter.

5 Please raise your tents.

6 Lance Hoffman?

7 MR. LANCE HOFFMAN: This question is for
8 Mischel. You -- I was very interested in your
9 discussion on the privacy training that you're -- you
10 put your people through. And there's obviously some
11 security training, as well. And I'd like you to,
12 maybe, expand on that a bit. Maybe if you -- maybe
13 you've provided us some information, or you could
14 provide some more information on -- more detail on what
15 you do, because what I'm looking at is the generality
16 of it. Is this something that could be generalizable,
17 or maybe already it is, beyond US-CERT, within DHS?
18 Also, the vectors of transmission, is it trained -- you
19 know, is it in person? Is it distance training? Is it
20 -- how do you do this? And is there any leveraging
21 that could be done with -- cooperating with other
22 agencies -- other entities, like the Privacy Office or

1 whomever?

2 MS. KWON: Well, I'm going to share with this
3 question with Pete, because, actually, Pete does the
4 training. The Privacy Office and OTC, our counsel,
5 together does the privacy and minimization training for
6 US-CERT. This training developed for us, and delivered
7 to us in person, and is quite a good training program.
8 So, maybe, Pete, you can -- you can take some of that.

9 MR. SAND: We do provide in-person training
10 for the entire US-CERT staff and anybody else who is
11 going to participate in this activity. And it covers
12 general privacy principles, an understanding of what
13 privacy is, and how it -- how it will show up in their
14 world. And then, we're going to build privacy training
15 specifically related to the issues that are going to
16 come up for them, drawing from the PIA.

17 Also, every employee of DHS has to go through
18 general privacy training, privacy awareness training,
19 and there are other online and in-person trainings that
20 everybody receives that, again, provide that
21 foundation. Some of those are online and some of those
22 are in person.

1 MR. LANCE HOFFMAN: Thank you. I didn't
2 realize this is basically the general Privacy Office
3 training, but particularized to US-CERT. Is that -- do
4 I have that right?

5 MS. KWON: Yes. I mean, it is general
6 privacy training, but it also digs down deep into the
7 technology that they're using and the actions that
8 they'll be taking, helps them identify PII and SPII and
9 U.S. persons information, teaches them about the
10 minimization procedures and the audit procedures that
11 we -- that we do. And it's quite comprehensive.

12 MS. SOTTO: Neville Pattinson?

13 MR. PATTINSON: Thank you, Lisa.

14 I'd like to thank all of you for coming in.
15 Terrific panel this afternoon. Very, very engaging.
16 I'd like to ask Steven how he sleeps at night, with the
17 -- with the alarming series of problems that we have on
18 our cyber security initiative. Clearly, there's a long
19 way and a lot of issues that we have to go. And having
20 now all of the 12 points of the recommendations, I
21 feel, you know, that we've got an action plan.

22 On one particular point, you have the

1 government-systems access points from four and a half
2 thousand it's producing now. This is great. What
3 about the five million people that access the government
4 systems? I think there's about five, five and a half
5 million, I saw from an OMB report recently. They're
6 all logging into the computer systems internally to the
7 Federal Government. How are we -- how are we
8 protecting that massive amount of potential social
9 engineering and all that user name and password access
10 risk?

11 MR. CHABINSKY: To -- your question, I think,
12 presents a very large issue for all of the industry, so
13 -- not just government access. When you think of the
14 banking and finance issues that we've been seeing, it
15 goes along the lines that you've displayed in your
16 question, which is, there are a lot of people whose
17 accounts appear to have been hacked into, when, in
18 fact, it's that there's a keystroke logger on the
19 consumer end which ends up having their password. And
20 the bank is perfectly secure, but there is some loss of
21 confidence, inappropriately so, to the bank, because it
22 appears that someone broke into the account, when it's

1 really on the consumer end.

2 I think the challenge that's before us, the
3 solution to that challenge, takes a couple of forms. I
4 think, predominantly, we've been going about it in two
5 ways. One is education. I think that the public is
6 becoming much more aware of social engineering issues
7 and spam issues and not opening up e-mails from people
8 you don't know. Of course, that's only part of the
9 problem, because you could get a spoofed e-mail from
10 someone you do know, and be in the same boat.

11 But, the other really -- the other side of
12 this really does have to be more of a technology fix,
13 and there are a lot of groups that are looking into,
14 you know, tokens and other ways to make sure that we
15 have identifiers for when we're using computer space.
16 But, there's not a simple answer to how you really get
17 safe computing practices to the masses. So,
18 fundamentally we've been relying, as well, on some of
19 the best industry practices that we've seen. So,
20 whether it's having to type in passwords, that you,
21 yourself, get to see, that are -- you know, that are
22 graphically altered, that a lot of the -- a lot of

1 industry is using now, those are the types of areas
2 that we're looking at.

3 But, the fundamental premise of your question
4 is a complex problem for us, that ultimately we don't
5 have security, as a nation, until we get to every home
6 user, because it's still -- it still is very much
7 dependent, not just on the technology, but on the user
8 end. And I think it's going to remain that way for
9 quite some time.

10 MS. SOTTO: Thank you.

11 Dan Caprio?

12 MR. CAPRIO: Thank you very much. This has
13 really been a very informative panel.

14 So, really, a question for you, Steven, and
15 that is, Can you talk a little bit more about the
16 privacy and civil liberties component of CNCI? For
17 instance, I mean, how are you incorporating the privacy
18 and civil liberties concerns within the -- within the
19 concept or the context of Project 12?

20 MR. CHABINSKY: If I could -- I would really
21 defer to Peter on Project 12, since that's a Department
22 of Homeland Security lead. So, let me --

1 MR. CAPRIO: Okay.

2 MR. CHABINSKY: -- take it up a level.

3 Congress asked, and we supplied to Congress,
4 a report from the Office of Director of National
5 Intelligence Civil Liberties and Privacy Office, which
6 reviewed the entire CNCI. So, at that level, the CNCI
7 was reviewed communitywide, or at least on behalf of
8 the community.

9 I would also say, Department of Justice, by
10 providing its legal analysis, also, therefore, provided
11 a privacy analysis, because it is impossible to review
12 these programs without relying on a review of those
13 laws that are in place to protect privacy. So, whether
14 it's our surveillance laws or our information-sharing
15 restriction laws, those have all been reviewed by the
16 Department of Justice, as well. And I think what
17 really is added by having the privacy focus, since so
18 much of this really is statutory and becomes legal
19 obligation, is not just issues that one would steer off
20 to the privacy person, but, fundamentally, these are
21 laws that would be broken, not complied with; it's not
22 -- these are must-haves that Department of Justice

1 looked at. I think where privacy has added a lot of
2 benefit really is in the compliance area, that
3 otherwise would not necessarily be mandated by law.
4 But, how do you ensure that you have proper compliance
5 and that areas that would include more optics review,
6 not just really the letter of the law, but how do you
7 make sure that there's confidence that the law is going
8 to be followed.

9 And so, the combination of having a strong
10 legal review throughout the program, in combination
11 with the privacy and civil liberties, I think, gives
12 you both the dynamics of steadfast observance of the
13 law, and then making sure that have a compliance
14 routine in place.

15 MR. CAPRIO: Peter, can you take the second
16 half, the Project 12? Because, I mean, Project 12, we
17 -- we've -- there's been a lot of discussion about it,
18 you know, in particular, among the IT community and the
19 different sectoral ISACs. But, is there -- is there a
20 plan related to outreach or the public/private
21 partnership on the privacy and civil liberties side?

22 MR. SAND: Well, we're working very closely

1 with the program office that's leading that, to make
2 that, when there are discussions that relate to that,
3 that we're involved and we're able to contribute and
4 ask the annoying questions that we ask, and make sure
5 that the concerns that we have related to the privacy
6 -- what information is being shared, what the -- what
7 the other concerns are on the other side of that, not
8 the government side, but the -- on the equivalent
9 structure side, that those are addressed and those are
10 incorporated into the overall approach. So, we work
11 directly with the program as they approach that.

12 MR. CAPRIO: I guess what I'm asking is,
13 maybe, a more formal mechanism, I mean, for outreach,
14 and intake, and input. And if there isn't, maybe it's
15 something that, you know, this committee might be
16 involved with or you might want to take --

17 MR. SAND: Our current --

18 MR. CAPRIO: -- under advisement.

19 MR. SAND: -- our current approach, at this
20 point, has been to stay closely tied to the program
21 itself and do the work as the program is doing the
22 work.

1 MR. CAPRIO: Okay, thanks.

2 MS. SOTTO: John Sabo?

3 MR. SABO: Yeah, that -- just to follow up on
4 that, it's been one of the criticisms from the private-
5 sector side, is obviously -- it was a classified
6 initiative, classified presidential directive, and only
7 Project 12 was, after about a year, opened up for
8 input. But, I think it's a valid point, that -- for
9 example, one of the obvious techniques in information
10 security is content inspection, that you're not simply
11 looking at packet information and flow, but you're also
12 looking at content, because an attack vector is
13 embedded content in a document. That may have been
14 addressed in the -- I don't recall that it particularly
15 was addressed in the Einstein 2 thing, because it may
16 not be an Einstein 2 component, but that type of thing
17 would lead to questions of -- well, how long are -- you
18 know, is this stored? Some content systems store the
19 data for a period of time for analysis, things like
20 that. So, it's a general comment.

21 The other thing is, Are there plans to deal
22 with issues in the CNCI, which I don't see -- you know,

1 I haven't seen in the recap of the 12 issues, per se --
2 on identity authentication and access controls?

3 Because when you start moving into identity systems and
4 authentication systems, which are also a component of
5 protecting our networks, you're now moving into data
6 which is personally identifiable, and which has the
7 potential for impacting our privacy and the privacy of
8 contractors, subcontractors, or citizens who make use
9 of these governmental systems. So, just a general
10 question, Is, you know, identity authentication and
11 access management addressed -- being addressed in CNCI?
12 And if it is, is there outreach -- or will there be
13 outreach to bodies like this, or others, that deal with
14 privacy implications of it?

15 I would make a comment that I'm -- I have
16 access to some of the US-CERT systems -- LLIS, a few
17 others -- personally. Everything is PIN and password-
18 protected, everything is stovepiped. There doesn't
19 seem to be any approach to using -- from the private-
20 sector side, like a FIPS-201 or some other standard
21 that would allow us to use a token or some standards-
22 based identity system. So, you know, it seems to me

1 that you're likely to be moving in the direction of
2 that standardization. The fusion center, we had
3 testimony about that a while ago. They're using
4 different systems. How is all that fitting together in
5 CNCI, the authentication, identity, and access
6 management piece? Can you talk about that or is that
7 classified?

8 MR. CHABINSKY: For internal government use,
9 that would be part of the conversation for protecting
10 our closed classified networks, the notion of identity
11 authentication and access controls. The CNCI itself
12 does not have a separate program that's looking at
13 identity authentication or tokens with respect to the
14 private sector or the citizens' use of government
15 services. So, that's still being continually looked at
16 on, I think, probably an agency-by-agency basis. I
17 wouldn't be surprised if there's a working group among
18 CIOs or the like that is looking at that project, but
19 that's not part of the CNCI.

20 MS. KWON: And, Steven, the unclassified
21 networks, the OMB 06/16 memo that Karen Evans
22 distributed, talks about two-form factor authentication

1 for government systems. And just as a note, the
2 [inaudible] portal for the government portion of the
3 portal is two-form factor token authentication.

4 MS. SOTTO: Reed Freeman?

5 MR. FREEMAN: Thank you, and -- Mr. Chabinsky
6 -- and thank you for your showing up. And I'm really
7 impressed by the rigorous thinking and planning that
8 your group has done.

9 I have one question, which comes from my
10 private-sector experience in data security. And in --
11 so, in reducing the access points down to, optimally,
12 100, my question is, How would you respond to two
13 criticisms I can imagine, and for which I assume
14 there's some consensus? And that is, there is no such
15 thing as perfect security. And the second is that the
16 fewer access points there are, the more interest there
17 is by a bad actor in each one. So, given those net--
18 net, are we more secure that way, or not?

19 MR. CHABINSKY: We did consider redundancy
20 and resiliency. Obviously, if you're going to be
21 reducing your points, you've obviously made each of
22 those more important and more targeted. I think that

1 our view of bringing it down to under a hundred is more
2 of a reflection of the bad state of affairs that we're
3 under today. So, now we have 4,500 networks that really
4 are being viewed as potential and actual targets, and
5 so, we've already lost the game, in that regard, with
6 the 4,500. So, this is not -- having seen the other
7 side, I think we were able to make the risk calculus
8 that bringing it down to somewhere under a hundred
9 would still provide enough redundancy and resilience,
10 and wouldn't make the problem or the persistence of the
11 threat actor greater. That interest exists. Our
12 networks are largely mapped; in fact, sometimes better
13 by our adversaries than by ourselves.

14 So, unfortunately, I don't believe we're
15 putting ourselves -- I say "unfortunately," because it
16 just shows where we are today, that our networks are
17 already under that microscope, and our adversaries are
18 already taking advantage of that. What's happening to
19 us now, I believe, is that we're just not seeing it,
20 not that it doesn't exist because we have so many
21 networks. And therefore, I really do believe that this
22 is the best plan. Certainly, that was considered.

1 And thank you for your earlier comments.

2 Appreciate that.

3 MR. FREEMAN: Thank you.

4 MS. SOTTO: Joanne McNabb?

5 MS. McNABB: Thank you very much, all of you.

6 I have a tiny suggestion, on the education
7 front, on reaching consumers. And this is probably
8 under Project 12, or Initiative 12. Online banking
9 sites currently provide information about identity
10 theft that is fairly prominently displayed now, "Watch
11 your wallet, don't answer a phishing e-mail," but they
12 don't provide information about securing your home
13 computer. So, here you've got people going to a site
14 who recognize they have a risk. It's a teachable
15 moment. If they provided good, simple information,
16 like what's on OnGuard Online, on the need to protect
17 your home computer to protect your bank account, that
18 might be a good opportunity. I suspect it doesn't
19 happen, because the banks don't want people to be
20 worried about it.

21 MR. CHABINSKY: We've seen the banking and
22 finance community actually step forward in a number of

1 regards. If you were to go to their websites, you
2 would certainly see information about socially
3 engineered e-mails.

4 MS. McNABB: Yes, and a whole lot of time on
5 how to recognize a phishing e-mail.

6 MR. CHABINSKY: And I think, quite frankly,
7 that there's a point where the ability to actually
8 defend your networks is a very fast-moving environment,
9 and I don't know that the banks believe that they're in
10 the best position to be as forward as you'd recommend
11 on telling their customer base how to secure their
12 systems. So --

13 MS. McNABB: But, they could lead them to OnGuard
14 Online.

15 MR. CHABINSKY: I'd -- I could take that
16 under advisement, and we certainly could have
17 conversations with them. I think it's a good point. I
18 think they've gotten engaged, to some extent, so
19 certainly they're thinking about the problem, but I
20 believe they've -- I can't speak for them, but it would
21 seem as though they've created a line of what they
22 think is appropriate for them, as an industry, to

1 impart. But, we have seen, certainly, a lot of
2 information on their sites about social engineering.

3 MS. KWON: And I do think it's a team -- like
4 I said, it's a team sport, and I think you could -- you
5 see efforts put by the ISACs to put out different
6 messages of that sort, do webcasts. InfraGuard also
7 does great webcasts and broadcasts and broadcast e-
8 mails about protecting your systems. Different websites
9 -- security websites -- I won't give plugs, so
10 -- but, different security websites also do the same
11 thing, our anti-virus vendors do similar things. So, I
12 think the encouraging news is that more -- you're
13 seeing more and more of this, and the team sport is
14 coming together. And, on the GFIRST public facing of
15 US-CERT website, we also give similar advice and point
16 you to similar websites that can give more advice.
17 So, you know, I think we need to encourage this team-
18 sport activity.

19 MS. McNABB: And the trick is getting to the
20 right people at the right place. That's why I'm
21 suggesting something other than government
22 communications channels.

1 MS. SOTTO: Ramon Barquin, I'll give you the
2 last word, but if you could make it fast, we're running
3 out of time. And I know we had at least one other
4 question for this panel. So, if you can stick around
5 for a little bit, I think there are at least a couple
6 of other questions for you.

7 Thank you.

8 DR. BARQUIN: As quick as I can do it.

9 So, as the -- as the power of devices, if you
10 will, the functionality that we're putting in them,
11 increases, there's going to be a lot more temptation to
12 target -- the iPhone of General Petraeus, specifically.
13 Now, you put, on the other side, again, the widespread,
14 now, diffusion of location-awareness devices, and I
15 start to see a potential situation arising, where we're
16 going to want to collect a lot of information that is
17 going to be very, very specific to the individual. And
18 again, on the one hand, you need it to protect; on the
19 other hand, there is the potential for significant
20 privacy events. So, again, a quick comment, because we
21 could spend all day or -- you know, talking about it,
22 but -- within CNCI --

1 MR. CHABINSKY: I think your comment, for --
2 as it would pertain to this group here, I think we will
3 start seeing -- this is really a projection, that
4 corporate America, as well as the government, will have
5 to start focusing more on its own employees and what
6 systems they were given, and keeping track of them. We
7 started doing that, because, quite frankly, at the
8 beginning, we were worried that we would lose your --
9 you know, someone would lose their laptop or their hard
10 drive or their thumb drive. So, just as a good
11 management practice, there was a lot of information
12 that was available of who owns what property. And I
13 would predict that your comment is on target, that
14 we're going to have to start looking at that, to start
15 seeing -- when we get the logging information, what is
16 the targeting, what can we -- what story can we tell?

17 And to further -- to further expand upon your
18 remark, there was a point -- there are some intrusion
19 series that we do look at where, all of a sudden, we
20 start seeing less exfiltration, meaning the quantity of
21 data is less than it had been, although the access to
22 data is the same or greater than it was. So, what does

1 that tell you? It tells you it's more targeted.

2 So, as our adversaries take greater control
3 of our networks, are able to better target what they
4 want, they don't have to do a smash-and-grab; they --
5 it's actually -- at first, I think, out of naivete,
6 when I looked at this, I said, oh, great, they only
7 stole 50 megabytes instead of two gigabytes. And then
8 the realization sunk in, that's actually not good news.

9 So, I agree that we are going to have to
10 start figuring out, at least on the -- on the
11 employee/employer relationship, how that's going to be
12 handled. There's nothing specifically that's, right
13 now, addressing that issue, as a specific matter. But,
14 again, to the greater point, I think, to step us back,
15 is that when we've been considering all of these
16 projects, no matter how high level -- or that when you
17 dive deep in and get it tactically and start acting,
18 there's been a very strong recognition by those who are
19 creating the plans, to include the lawyers and the
20 privacy folks. And that's the good-news story. This
21 is not an afterthought, in perhaps the way it would
22 have been ten years ago. This has become an ingrained

1 view. So, the work that you have been doing and that
2 the community has been doing is more and more becoming
3 the fabric of how government works; and the outliers,
4 fortunately, become when people didn't consider
5 privacy, not when they did. So that, I believe, is a
6 good-news story.

7 MS. SOTTO: Okay. Thank you so much. This
8 was a fascinating panel for us. And we've been wanting
9 to hear from you for a long time, and really appreciate
10 your joining us.

11 Public comments?

12 MR. HUNT: Yeah, I'm not -- our Federal
13 Register Notice did mention that we would allow members
14 of the public to make a three minute presentation to the
15 committee, if they wish. Otherwise, members of the
16 public can always submit things to me that I will
17 forward to the committee.

18 And a transcript of this -- of this meeting
19 will be made available and posted on our DHS Privacy
20 website in the future. And I have also spoken to them
21 about trying to get certain portions faster, and we'll
22 see if we can make that -- make that arrangement, as

1 well.

2 Are there any members of the public who are
3 interested in addressing the committee?

4 [No response.]

5 MR. HUNT: I'll take that as a no. And
6 without further ado, I think we're adjourned. Look for
7 our next meeting in -- February, I think was discussed.
8 That is subject to change, but it's at least our
9 initial -- our initial plan.

10 Thank you very much, to the panelists and to
11 the whole committee. This was a fantastic meeting.

12 Thank you.

13 [Whereupon, at 3:55 p.m., the meeting was
14 adjourned.]

15

16

17

18

19

20

21

22