

1 DEPARTMENT OF HOMELAND SECURITY
2 MEETING OF THE
3 DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

4
5 Wednesday, March 9, 2011
6 Carl Hayden
7 Conference Room
8 U.S. GPO Building
9 732 North Capitol
10 Street, N.W.
11 Washington, D.C.

12
13 The meeting was convened, pursuant to notice, at
14 1:01 p.m., RICHARD V. PURCELL, Chairman, presiding.

15
16
17
18
19
20
21
22

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

COMMITTEE MEMBERS PRESENT:

RICHARD V. PURCELL, Chairman, presiding

- | | |
|----------------------|-----------------------|
| ANA I. ANTON | RAMON BARQUIN |
| J. HOWARD BEALES III | DANIEL W. CAPRIO, JR. |
| JAMES W. HARPER | DAVID A. HOFFMAN |
| LANCE HOFFMAN | JOANNE McNABB |
| NEVILLE PATTINSON | LAWRENCE PONEMON |
| JOHN SABO | LISA J. SOTTO |

ALSO PRESENT:

MARTHA K. LANDESBURG, Executive Director
and Designated Federal Official

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

2 MS. LANDESBURG: Ladies and gentlemen, if you'll
3 take your seats, please. We're going to begin the meeting.
4 Thank you.

5 Welcome to the first quarterly meeting of the DHS
6 Data Privacy and Integrity Advisory Committee. I am Martha
7 Landesberg, the Designated Federal Official. With that, I
8 am going to turn the meeting over to the Chairman, Richard
9 Purcell.

10 CHAIRMAN PURCELL: Thank you, Martha.

11 Thank you for being here, committee members.
12 Thank you for joining us today. We look forward to another
13 exciting meeting. The first things we always mention and I
14 will mention as always are the need for courtesy by
15 silencing your digital devices in ways that prevent us from
16 being disturbed in our deliberations by their incessant
17 ringing.

18 We also want to remind members of the public here
19 that comments from the public are taken at 4:00 o'clock this
20 afternoon to 4:30. If you have an interest in addressing
21 the committee at that time, we'd encourage you to sign up at
22 the table outside this room and we look very much forward to

1 hearing as many comments as we have. It looks like we'll
2 have -- we have a crowd today. This is good. We'd like to
3 hear more from the public about the deliberations, either
4 the deliberations we conduct today or questions you might
5 have in the future.

6 A reminder: If you do have questions of any of
7 the members of the committee that you aren't able to ask or
8 of the witnesses that you're not able to address because
9 they'll be testifying and then going, please feel free to
10 write to the Privacy Office. Martha Landesberg, our
11 Designated Federal Official, will take those requests and
12 she will channel them and make sure that your query is
13 delivered to the proper person and that you have a response
14 to it.

15 So with that, I'd like to welcome once again Mary
16 Ellen Callahan, the Chief Privacy Officer of the Department
17 of Homeland Security. Mary Ellen is our tutor, our mentor,
18 and our instructor in many ways. Prior to joining DHS, Mary
19 Ellen specialized in privacy, data security, and consumer
20 protection law as a partner at Hogan and Hartson here in
21 Washington, D.C. She also has served as Co-Chair of the
22 Online Privacy Alliance and was Vice Chair of the American

1 Bar Association's Antitrust Division Privacy Information
2 Security Committee.

3 Mary Ellen's job as Chief Privacy Officer includes
4 the DHS Privacy Office team, a group of sterling talent that
5 she and others have put together over the years. She is
6 responsible for privacy compliance with that office across
7 the entire Department spectrum and also serves as the
8 Department's Freedom of Information officer.

9 She celebrates her second anniversary now as the
10 Chief Privacy Officer, and on behalf of the committee I
11 congratulate you, Mary Ellen, on two very productive years,
12 and we look forward to lots more accomplishments and sharing
13 of information as the tenure continues.

14 So we're eager to hear about your office's
15 activities since the last time we met, so please proceed.

16 DHS PRIVACY OFFICER UPDATE,

17 BY MARY ELLEN CALLAHAN

18 MS. CALLAHAN: Thank you very much, Mr. Chairman.
19 It is hopefully a good omen that this is indeed exactly my
20 second anniversary. So I am looking forward to updating the
21 committee on many of my activities and my office's
22 activities.

1 I also wanted to remind the committee and the
2 attendees that I'm pleased to say that Howard Schmidt, the
3 Special Assistant to the President and Federal Government
4 Cybersecurity Coordinator, will follow me with an update on
5 the Obama administration work on cybersecurity. We are very
6 honored to have Mr. Schmidt with us today.

7 And continuing our series of briefings from DHS
8 component privacy officers, we'll ask Donald Hawkins, the
9 privacy officer for the U.S. Citizenship and Immigration
10 Services, to discuss the USCIS's implementation of
11 privacy policy and compliance.

12 Last but certainly not least, our own Eric Leckey,
13 the Associate Director for Privacy Compliance and Program
14 Development in my office, will brief you on efforts to embed
15 privacy protections in the Department's use of social media
16 and will also answer Ramon's question from last time about
17 the formal establishment of the DHS Data Integrity Board.

18 So with that said, if I could turn to the
19 accomplishments, ongoing activities, and future plans that
20 the Department has been up to, and we have been busy.
21 First, in terms of staffing we continue to grow. I assume
22 that growth may end some time soon, but that's okay because

1 we've got a great staff, and we've got a great team among
2 us.

3 Debbie Diener, who joined us in September as our
4 new Senior Adviser for Director of Privacy Policy, is
5 already deeply immersed in many of the DHS and
6 intergovernmental privacy policy issues, several of which
7 I'll discuss later on. She has actually recently been
8 joined, last week, by Charlie Cutshall, who formerly has
9 served as a DHS policy fellow in our office and now has
10 joined as the most recent member of the DHS privacy policy
11 team. So we welcome Charlie and appreciate his cooperation,
12 his contributions.

13 Kate Claffie has joined us as the first Associate
14 Director of Privacy Incidents and Inquiries. She came to us
15 from the FTC, where she was a senior investigator working on
16 privacy and identity theft issues.

17 Scott Mathews, our new Senior Privacy Analyst for
18 Intelligence, joined us last month from the Commerce
19 Department. And Deborah Danisek has come to us from the
20 State Department to round out a new combined team that I'll
21 detail momentarily.

22 Furthermore, with the addition of two FOIA

1 specialists and one administrative specialist, we are
2 essentially fully staffed on the FOIA side.

3 So to give a big picture of how much we've grown
4 since I've started, of the 25 new staff members that have
5 come on board since I've become Privacy Officer, part of
6 those increases are related to -- we have reduced our
7 expenditures from contractors from 26 percent of our FY '09
8 budget to 4.5 percent of our budget currently. Therefore we
9 have used our resources that were formerly allocated to
10 contractors to hire 17 new FTEs, 9 privacy, 5 FOIA, and 3
11 administrative -- I think it's actually 9 FOIA, 5 privacy,
12 and 3 administrative staff. So we've really been able to
13 bolster our federal employees in order to develop the office
14 and to further the office.

15 Some have commented that they get lots of
16 announcements about jobs as a member of the DPIAC for the
17 Privacy Office and I wanted to explain that that was due to
18 the Director of Administration and the Deputy Chief FOIA
19 Officer's and my strategic decision to convert those
20 contracts. So we're very thrilled to have everyone on
21 board.

22 I mentioned that we have a new team or a new

1 office. So one of the things I've done while expanding the
2 office is to enhance the efficiency and the impact of my
3 office's work. I recently formed the Privacy Information-
4 Sharing and Intelligence Group. There is a debate on the
5 pronunciation of that team. Those of us in the know call it
6 "PISS-ie." Those of us who have a more international bent
7 try to call it "PEE-zay."

8 (Laughter.)

9 Perhaps my deputy really doesn't like to say the
10 word "PISS-ie," but I do.

11 The PISI group is actually a great combination of
12 staff who are working in information sharing, fusion
13 centers, and reviews of the DHS Office of Intelligence and
14 Analysis reports and projects, and I have been briefing you
15 on these various and sundry elements. What we've done is
16 we've formed this team with Scott Mathews and Deborah
17 Danisek, the two new additions I mentioned, along with Helen
18 Foster, who has briefed this committee, and of course Ken
19 Hunt, who has been working on these issues quite a long
20 time.

21 With regard to information sharing, the
22 Information Sharing Inter-Agency Policy Council, the ISAIPC

1 -- and maybe we should keep track of all the acronyms I use
2 today -- has been reorganized under the joint chairmanship
3 of the national security staff and the program manager of
4 the information sharing environment. As part of that
5 reorganization, the ISE Privacy and Civil Liberties
6 Guidelines Committee has been reformatted to be a
7 subcommittee under that inter-agency policy council. As I
8 had formerly done with the Privacy Guidelines Committee, I
9 co-chair this group, now known as the Privacy and Civil
10 Liberties Subcommittee, with the privacy and civil liberties
11 officers of DHS, ODNI, and Department of Justice.

12 The subcommittee will continue to provide privacy
13 and implementation guidance for sharing of terrorism
14 information in the federal community.

15 The ISAIPC also formed additional subcommittees
16 dedicated to information sharing environment priorities,
17 including fusion centers, suspicious activity reporting,
18 watch listing, and information integration. I have assigned
19 Privacy Office staff to each of those subcommittees.

20 As you heard in the September meeting, we -- and
21 in fact we've heard a couple of times -- last year DHS tied
22 to continuing use of DHS grant funding with a requirement

1 that all fusion centers have a written privacy policy that
2 is at least as comprehensive as the ISE privacy guidelines.
3 The tying of the grant money was to indicate that after 6
4 months after receiving the grant money you could no longer
5 receive or use that money unless you had a privacy policy
6 that was indeed approved by me personally in my capacity as
7 a co-chair of the Privacy and Civil Liberties Subcommittee.

8 I do review each privacy policy before it's final
9 and the review is at the end of a long technical assistance
10 program run by the Department of Justice Bureau of Justice
11 Assistance. I'm happy to announce that as of today, as of
12 tonight probably after I sign the last letter, I have issued
13 letters to 65 of the 72 fusion centers certifying that their
14 policies meet the ISE requirements. The rest of the centers
15 are busy finishing their policies and we're prepared to
16 review them with a quick turnaround as they come, because
17 the deadline for the end of the funding is the end of this
18 month. But we are quite close to the goal and I anticipate
19 that I will likely approve 68 of the 72 by the end --
20 actually, hopefully by the end of this week, if not the end
21 of this month. Four centers are not -- are still in a
22 fledgling status, so they may not have completed privacy

1 policies. But we have more than met that goal, and I'm
2 quite proud of the work that Ken Hunt has done in the
3 leadership on those issues.

4 With regard to fusion centers, we continue to be
5 quite active training I&A intelligence professionals along
6 with CRCL before they're assigned specifically to a fusion
7 center. Furthermore, since our last meeting the Privacy
8 Office, together with the DHS Office for Civil Rights and
9 Civil Liberties, has traveled to fusion centers in North
10 Carolina, South Carolina, New Jersey, Delaware, Oklahoma,
11 Alabama, and Mississippi to give that in-depth, in person
12 training to the entire fusion center as part of our
13 continuing support for fusion centers, and we have completed
14 our training of the train the trainer elements for the
15 privacy and civil liberties officers that we discussed and
16 focused a great deal of attention to last calendar year.

17 The in-depth training should likely continue.
18 It's of course a resource-intensive program. But we're
19 committed to visiting as many centers as possible to give
20 this in-depth training or continuing to support the privacy
21 and civil liberties officers as they develop their own
22 training going forward.

1 For the fourth year in a row, the Privacy Office
2 will participate in the National Fusion Center Conference
3 next week in Denver. I am scheduled to address the center
4 directors the day before the conference begins. This will
5 be an opportunity to congratulate those centers that have
6 finished their privacy policies and also to speak with those
7 few centers that have not yet completed them in order for
8 them to provide their immediate attention to this issue,
9 while encouraging all of the directors to continue to build
10 privacy and civil liberty protections into their work going
11 forward.

12 During the conference itself, I'm appearing on a
13 panel on building a culture of privacy within a fusion
14 center, and there I'll stress the importance of investing in
15 the privacy program. I'll also listen to their ideas on how
16 their federal program partners can assist the fusion centers
17 in honoring the public commitments in their privacy policies
18 and how to do so in a transparent way.

19 I'm now turning to the I&A product reviews that
20 I've discussed several times in the DPIAC. The PISI group
21 has reviewed -- and it really was the group because Scott
22 has just come on board about 6 weeks ago. They've reviewed

1 and cleared 77 intelligence products and 183 homeland
2 intelligence reports since the committee last met, and the
3 Privacy Office's responses were all provided within 48 hours
4 and met all the deadlines provided by the Office of
5 Intelligence and Analysis.

6 Since we've last met, we have been extraordinarily
7 productive in our guidance and reporting, and I wanted to
8 kind of detail some of those and we'll talk about them more
9 in a little bit. In December we submitted our fifth
10 comprehensive Data Mining Report to Congress. In January we
11 published -- and in fact we were the first Department to
12 publish online -- the FY '10 Annual FOIA Report to the
13 Attorney General, the results of which I'll detail in a
14 little bit. And today we'll publish the follow-up report on
15 that, which is the 2011 Chief FOIA Officer's report to the
16 Attorney General, which focuses more on the Department's
17 transparency and open government initiatives.

18 Also in February, we released the Privacy Policy
19 Guidance Memo on Privacy Act Amendment Requests, which is in
20 the packets of the members and is available outside. This
21 document sets forth component privacy officers' and FOIA
22 officers' responsibilities for identifying, processing,

1 tracking, and reporting on requests for amendment of records
2 under the Privacy Act.

3 The guidance was a joint effort of our Policy,
4 FOIA, Compliance and Incidents and Inquiries groups and will
5 help provide guidance for officers throughout the Department
6 on how to identify amendment requests and address them
7 appropriately.

8 We've also revised several sections of our
9 Handbook for Safeguarding Sensitive Personally Identifiable
10 Information to clarify employees' responsibilities for
11 securing PII when not in use.

12 And just last week I released my first public
13 report under my investigatory authority activities, titled
14 "OIG Privacy Incident Report and Assessment." I'll have
15 more to say about that in a minute.

16 I'm also pleased to tell you that at long last --
17 and there are several members in this audience who will be
18 happy about that -- the FY 2011 Homeland System grant
19 guidance and application kit will include a section on best
20 practices for the collection and use of PII, recommending
21 that all grantees have a publicly available privacy policy
22 and that grantees use our new PIA guidance and template to

1 develop their own privacy policies. Thank you.

2 Copies of the most recent documents are in your
3 folder and I'll refer to them during the rest of my
4 presentation. And as always, they of course are always
5 available on our web site, dhs.gov/privacy.

6 We have also been very active in the international
7 privacy policy realm, specifically engaged in the PNR
8 negotiations that the Deputy Secretary of the Department of
9 Homeland Security has been part of. Those talks are ongoing
10 and I'll have a more updated discussion of the PNR
11 negotiations in May. Hopefully I'll have a final update on
12 those negotiations.

13 In addition, we've been engaged generally with the
14 EU Justice and Home Affairs meetings. For example, in
15 December Lauren Saadat and I attended the JHA ministerial in
16 Washington, co-led by Secretary Napolitano and Attorney
17 General Holder, and for the EU Commissioners Redding and
18 Malmstrom. Privacy issues, such as PNR and the umbrella
19 data privacy agreement negotiations, were of course high on
20 the agenda.

21 Canada has also been a major area of focus for us,
22 as the Department looks to enhance cooperation in several

1 core mission areas. On November 16 and 19 in Toronto and
2 then Washington, D.C., respectively, I was joined in
3 Washington by our own Mr. Jim Harper. I participated in two
4 press events for the launch of the November issue of the
5 Wilson Center's Canada Institute publication "One Issue, Two
6 Voices," in which I wrote about privacy and information
7 sharing at the border. A copy is in your folders or also
8 available outside.

9 Furthermore, as a result of the announcement by
10 the President and the Prime Minister of Canada on the U.S.-
11 Canadian perimeter security declaration last month, February
12 11, I anticipate close cooperation with our Canadian
13 counterparts in the coming months as the governments of the
14 U.S. and Canada seek to expand cooperation on immigration,
15 counterterrorism, and law enforcement.

16 We also maintain our key role in the U.S.
17 government inter-agency group by participating in the OECD
18 Working Group for Information Security and Privacy meetings,
19 where we promote U.S. government positions that will lead to
20 OECD review outcomes consistent with U.S. law and best
21 practices. To demonstrate the practical effect of the OECD
22 guidelines, we partially funded a study by the Privacy

1 Projects on public sector application of the guidelines in
2 the U.S., Spain, Japan, Australia, and Canada. That study
3 was released in December and distributed through the working
4 party, and of course again it is in your folder or available
5 on our web site and also out there. And I wanted to thank
6 Richard Purcell for his work on that project.

7 We've done also other international outreach that
8 some of you are familiar with, including presentations at
9 the International Conference for Data Protection and Privacy
10 Commissioners in Jerusalem in October, briefings related to
11 preventing and combatting serious crimes, as well as
12 discussions on the EU-U.S. data protection agreement that I
13 mentioned earlier.

14 With regard to compliance, we've been very active
15 in that as well, having processed 22 privacy impact
16 assessments, 224 privacy threshold analyses, 6 computer
17 matching agreements, 5 SORNs, and 2 notices of proposed
18 rulemaking, and 1 final rule to implement Privacy Act
19 exemptions.

20 In addition, since the last meeting DHS has
21 improved its FISMA privacy score for PIAs by 6 percent to 76
22 percent since the end of FY 2010. Our goal is to reach 80

1 percent by the end of 2011 and I believe that we're well
2 within the goal and within the target for doing so.

3 Programs for which documentation has -- programs
4 for which documentation was approved during this time
5 include: suspicious activity reporting, including
6 component-level suspicious activity reporting; the
7 Department's ISE SAR initiative and its participation in the
8 nationwide SAR activity reporting initiative; TSA's
9 automated imaging -- advanced imaging technology update; the
10 E-Verify self-check, which is set to launch on March 21 in
11 selected areas. We will also have a PIA for that, to be
12 launched very shortly.

13 I mentioned the National SAR Initiative. I want
14 to spend a little bit of time on that if I may. DHS is a
15 participant in the Nationwide Suspicious Activity Reporting
16 Initiative, to establish a unified process for reporting,
17 tracking, and accessing suspicious activity reporting
18 related to terrorism in a manner that protects privacy,
19 civil rights, and civil liberties. The NSI establishes a
20 nationwide component to gather, document, process, analyze,
21 and share information about suspicious activities, to enable
22 rapid identification and mitigation of potential terrorist

1 threats.

2 The capacity provides for authorized participants
3 to both contribute and search for SARs that are related to
4 terrorism, referred to as ISE SAR, in the NSI shared space,
5 provided that the activities be reasonably indicative of
6 terrorism or criminal activity associated with terrorist
7 behavior.

8 The Privacy Office has taken substantial steps to
9 minimize privacy impacts associated with the DHS ISE SAR
10 initiative through the publications of SORNs and PIAs that
11 discuss broader component SAR activities, as well as DHS's
12 participation in the NSI. We have published the DHS ISE SAR
13 initiative PIA last November. The PIA outlines privacy
14 risks as well as mitigation techniques. The compliance
15 group will conduct one of our ongoing privacy compliance
16 reviews that Jamie Pressman briefed you guys on last time,
17 related to DHS's participation in the NSI, in the fall of
18 2011.

19 A little plug if I may. Tomorrow I will be
20 speaking at an IAPP networking panel on privacy and civil
21 liberties protections in the NSI.

22 Our policy group, again led by Debbie Diener, has

1 been similarly engaged in efforts to embed privacy in the
2 DHS programs and in inter-agency efforts. We're active
3 participants in DHS and intergovernmental groups working on
4 identity management issues. This includes supporting me in
5 my role as a voting member of the DHS Identity Credential
6 and Access Management Executive Steering Committee. Debbie
7 Diener co-chairs the CIO Council's Privacy Committee on
8 Identity Management Subcommittee along with the FTC, Kellie
9 Cosgrove, Kellie Cosgrove Riley. The subcommittee is
10 actively engaged in an array of identity management issues,
11 including vetting privacy requirements and guidelines in
12 numerous documents associated with the federal identity
13 access and management roadmap.

14 Martha Landesberg, our Associate Director for
15 Privacy Policy, co-chairs the Privacy Committee's Best
16 Practice Subcommittee, which has undertaken an ambitious
17 agenda of projects aimed at providing guidance of state of
18 the art privacy practices for federal agencies. The policy
19 group has of course been working closely with our privacy
20 technology group on several biometric-related projects,
21 including: enhancing the availability of information on the
22 government's use of biometrics through a biometrics.gov web

1 site; and working with CRCL and the Science and Technology
2 Directorate to further develop internal guidance on the use
3 of biometrics.

4 Our Privacy Technology Group continues to develop
5 policies to address privacy issues associated with the
6 Department's various uses of technology. Since the
7 committee last met, my office, the Office of Civil Rights
8 and Civil Liberties, and the Office of General Counsel have
9 been staffing the new DHS Office of Cybersecurity
10 Coordination located inside the National Security Agency.
11 We're currently focused on building relationships with NSA
12 and DOD privacy and compliance staff. We also continue
13 working closely with Emily Andrew, NPPD's privacy officer,
14 to develop a strategy on how to best conduct Privacy Impact
15 Assessments of various DHS cybersecurity programs.

16 I also wanted to mention that NPPD together with
17 the Office of Policy is engaged in developing a unified
18 cybersecurity strategy for U.S. government civilian networks
19 and private sector networks under the DHS Quadrennial
20 Homeland Security Review. You have in your folders the
21 terms of reference for this strategy, which make it clear
22 that protecting privacy and civil liberties is embedded in

1 the strategy by design. We'll continue to keep you informed
2 on the progress of this important project.

3 Our privacy team, I know several of you will be
4 happy to hear, is also working very closely with the Office
5 of the Chief Information Officer to develop policies that
6 address the new challenges posed by the service model the
7 Department wants to use for IT service system development
8 and deployment. We're building on the Committee's previous
9 guidance on service-oriented architecture to create a
10 privacy compliance model that will enable DHS to be both
11 technologically agile and privacy compliant. Therefore, the
12 Department continues to benefit -- thank you very much --
13 from the Committee's 2010 recommendations on the PIA process
14 for the enterprise service bus development, and we are
15 working closely with the Department's newly created SOA
16 working group. We've decided to focus on services now to
17 stay aligned with the working group's agenda and will turn
18 to the infrastructure, to the enterprise service bus, next.

19 As detailed more fully in my 2010 reports, the
20 FOIA team has made extraordinary progress in reducing the
21 backlogs both of requests and of appeals. DHS processed
22 138,651 FOIA requests in FY 2010. I think it's actually 26

1 percent of all FOIAs that were provided to the federal
2 government in 2010.

3 The Department's open government plan was to
4 reduce the overall FOIA backlog by at least 15 percent and
5 we were anxious about meeting that, given a 30 percent spike
6 in incoming requests. So incoming requests was 130,098.
7 Thanks to the hard work of my office, the FOIA office, as
8 well as FOIA officers throughout the entire Department, we
9 were able to reduce the backlog by roughly 40 percent,
10 ending FY 2010 with a backlog of 11,383 requests in total.
11 The FOIA backlog when I started was 86,000.

12 As you know, my office processes FOIA requests for
13 DHS headquarters office. We reduced our backlog itself by
14 31 percent, from 22 at the close of FY '09 to 15 at the end
15 of FY 2010. The USCIS, ICE, Offices of Policy, Operations,
16 Management, and Inspector General also made significant
17 efforts and we've been able to reduce backlogs by --
18 backlogs of appeals, excuse me, from 2747 in FY '09 to 704
19 to the end of FY '10.

20 So I want to thank in particular CIS that reduced
21 its appeals backlog by 98 percent, and CPB completely
22 eliminated its FOIA appeals backlog. So they've done really

1 yeoman's work on these types of issues.

2 We've talked about Inquiries and Incidents before.
3 Just to give you an idea of the pace of our work, we had 115
4 privacy incidents reported since our last meeting. 82 of
5 these have been investigated -- 82 percent, excuse me --
6 have been investigated, mitigated, and closed. The rest
7 remain open and are being processed.

8 As you know, the 9-11 Commission Act expanded my
9 responsibilities to include explicit investigatory
10 authority, the power to issue subpoenas to outside agencies,
11 to nongovernmental agencies, the ability to conduct regular
12 reviews of privacy implementation, and greater coordination
13 with the Inspector General. At the last meeting I told you
14 I had invoked this authority to initiate an investigation
15 into a privacy incident that affected several components and
16 triggered multiple privacy and security concerns. My report
17 on this incident, which involved the Office of the Inspector
18 General and its contractor KPMG, has been published and a
19 copy of that is available in your folders.

20 The report makes findings and recommendations
21 addressing compliance with privacy policies and recommends
22 steps for mitigation, prevention of similar privacy

1 incidents across the Department, but also specifically when
2 dealing with cross-component elements.

3 Steve Richards briefed you guys in the fall and we
4 are continuing to develop the mandatory privacy training
5 that he discussed with you at that time. The request for
6 proposal will be out very soon and we hope to launch this
7 new interactive course later this year, replacing the
8 current "Culture of Privacy Awareness" course.

9 We are also currently developing a best practices
10 web site on the OMB Max portal for federal employees as part
11 of our work with the CIO Council's Privacy Committee.

12 I also continue my Privacy Information for
13 Advocates meetings. At our last meeting on December 17,
14 2010, we discussed FOIA issues. The next meeting is in 9
15 days on March 19 -- March 18, excuse me. No topic is
16 specifically identified, but we're certainly open to the
17 wide-ranging conversation that we always have during the
18 Privacy Information for Advocates meeting.

19 With that news, Mr. Chairman, that concludes my
20 report.

21 CHAIRMAN PURCELL: Thank you, Mary Ellen. That's
22 excellent. We're glad to hear particularly the development

1 of the staff, the conversion to federal employees away from
2 contractors. We think that the institutional knowledge
3 you're developing is going to pay long-term dividends both
4 for your office and for the federal privacy environment
5 itself.

6 I had one question I'd like you just simply to
7 expand on a little bit. The biometrics.gov initiative is of
8 course very interesting. Could you talk about what that
9 means in terms of the types of biometrics that are intended
10 to be captured and retrieved through that, but also more
11 specifically the Department's approach to DNA analysis in
12 that context?

13 MS. CALLAHAN: Absolutely. The biometrics.gov
14 idea is actually basically just a transparency initiative to
15 centralize and disclose what different departments are doing
16 with biometric initiatives, whether they be currently in the
17 research mode or whether they be in the implementation
18 phase. The idea was to have PIAs and system of records
19 notices up and available in a centralized fashion. We are
20 still investigating whether or not other departments are as
21 developed or transparent with their privacy impact
22 assessments on these issues.

1 So I don't know if it's necessarily -- there has
2 been a longstanding recommendation to develop this
3 centralized site. I don't know if it's feasible yet. So
4 we're still looking at that and working with different
5 inter-agency groups to do that.

6 With regard to the Department's use of --
7 specifically, I'll talk about the Department's use of DNA.
8 There was a question about a program that is in again a
9 research phase from the Directorate of Science and
10 Technology. The Directorate of Science and Technology, of
11 course, works on specific statements of work to try to
12 determine whether a use of any product that may be involved
13 would be -- is feasible in a confined area, confined
14 research area, and whether or not we can extrapolate and use
15 that in an operational area.

16 The Directorate of Science and Technology is
17 looking into a statement of work on trying to use, in a
18 voluntary fashion, use DNA to match to identify refugees who
19 may or may not have familial relationships. It's in the
20 very early stages and it's, as I said, in the research
21 capacity and would only be used on refugees that were
22 seeking to definitively establish a parent-child

1 relationship.

2 CHAIRMAN PURCELL: Thank you very much.

3 MS. CALLAHAN: And that's the only -- that's the
4 use of DNA with regard to the Department.

5 CHAIRMAN PURCELL: I guess just as one follow-up,
6 we hear about S & T's activities fairly frequently, and of
7 course some news emerges every once in a while. I think
8 that what occurs to me is to ask the question -- the concept
9 of privacy by design is an emerging foundational concept
10 within privacy program development. Can you explain to the
11 committee how privacy by design is being adopted and
12 implemented in the Privacy Office today?

13 MS. CALLAHAN: Absolutely. Privacy by design is
14 exactly the concept of making sure that we are involved
15 early and often with the program managers, with those who
16 are developing the program, and to make sure that the
17 privacy protections are embedded into the original design of
18 the program, to make sure that is part of the concept.

19 In fact, that's one of the reasons why I
20 recommended to the Deputy Secretary that the Directorate for
21 Science and Technology have a privacy officer and have one
22 directly. I was thinking, not to throw Mr. Chris Lee under

1 the bus, but it may be useful to have Chris be the next of
2 the component officers to come and talk to you about his
3 work with the directorate and particularly with the human
4 factors portion of science and technology, to make sure that
5 the privacy office at S & T is involved and integrated.
6 Actually, Chris works very closely with our privacy
7 technology group to make sure that the Department privacy
8 office is also aware of what the research projects are.

9 I'm not trying to say that Science and
10 Technology can engage in research activities that would not
11 have privacy protections. In fact, the opposite is true.
12 We want to make sure that the research that's being done has
13 the privacy protections embedded within it, and that's the
14 work of Chris and the privacy technology team with Pete Sand
15 and Liz Lyons, so that when it gets into being considered
16 even for an operational phase we understand that the
17 protections that are within it are ones that can scale.

18 CHAIRMAN PURCELL: Excellent. And Chris is the
19 bus driver. I'll be careful. But we welcome the testimony
20 in an upcoming meeting from S & T. It's an area of keen
21 interest by all the committee members.

22 With that, I'll turn to John Sabo first, please.

1 MR. SABO: Thank you.

2 Just a quick question. You've done so much work
3 on negotiating the PNR, data transfers, and so on, I
4 presume. So the question goes to the reciprocal issue,
5 which is EU member states, the EU, other countries,
6 beginning to collect U.S. biometric and passenger
7 information, which obviously as U.S. citizens we're not
8 necessarily protected under their laws.

9 Having said that, who would play the role of
10 looking at the interests of U.S. citizens? Would that fall
11 into your jurisdiction? I realize that may be a stretch.
12 But could you speak to that and whether or not you've been
13 speaking to these other data protection commissioners about
14 collecting our data?

15 MS. CALLAHAN: We certainly are very conscious of
16 that as a concern, about other countries collecting U.S.
17 information and what their uses and what their opportunities
18 for transparency and redress are. So since I've been here,
19 we actually have been attempting to be more bilateral in our
20 discussions, negotiations, and actually also trying to find
21 out what exactly other countries are doing, because the
22 interesting thing is I know more about what some European

1 countries are doing with data than perhaps people within
2 that country are doing.

3 So I think that even the European Parliament will
4 say that the U.S. government is much better on transparency
5 than perhaps some of their other areas are.

6 So, John, to answer your question about have we
7 identified this as an issue, absolutely. It is relevant and
8 has been incorporated into the PNR conversations as well as
9 the umbrella data protection agreement that is at a more
10 fledgling stage, and that from a -- the privacy committee
11 and specifically the international subcommittee of the
12 privacy committee would be the vehicle in which to address
13 that. Nancy Libin, the DOJ privacy and civil liberties
14 officer, and I engage in most of the outreach, so that's
15 where it would be, to try to figure out.

16 The interesting question is, some data protection
17 commissioners don't have authority over federal agencies
18 within their own government. So there may be some areas
19 where there isn't necessarily coverage. And we're trying to
20 narrow that down.

21 MR. SABO: Just a quick follow-up. Are we
22 handicapped in any way because we don't have a U.S. data

1 protection commissioner, or do you feel adequately
2 protected?

3 MS. CALLAHAN: I actually think that we're doubly
4 or maybe triply protected. We've got the work that I do
5 every day and the work that my staff does every day. We
6 certainly have the Office of the Inspector General, who goes
7 and checks these things out on the individual complaint
8 level, and then also of course more comprehensively as part
9 of their inspections, audits, and investigatory authority.
10 And we have the Government Accountability Office, as well as
11 the U.S. Congress.

12 I mean, the level of kind of review and process
13 from the individual complaint all the way up to the systemic
14 elements I think is incredibly comprehensive. I think I've
15 been part of, I think the number is, seven -- I think our
16 office in some element has been involved in seven IG
17 investigations or inspections and four or five GAO reviews
18 in my time.

19 CHAIRMAN PURCELL: Thank you.

20 Joan.

21 Ms. McNABB: I like the sound of what you said
22 about the grants process and look forward to seeing very

1 specifically what it says, because I think it is really
2 important that as the millions and millions and millions of
3 dollars roll out to the states they aren't just being used
4 to create a bigger surveillance network without any
5 consideration, and I appreciate the training that's been
6 going on as well.

7 But I heard you say E-Verify, that something is
8 about to happen on March 21st.

9 MS. CALLAHAN: The self-check. Sorry. I skipped
10 over that. I skipped over that paragraph --

11 Ms. McNABB: What is it?

12 MS. CALLAHAN: -- because I was running late.

13 Ms. McNABB: But what is it?

14 MS. CALLAHAN: That was my mistake. The E-Verify
15 self-check is a way of having an individual check their own
16 employment eligibility status prior to having their employer
17 do it. So if you were starting a new job, which I hope you
18 don't do, if you were starting a new job and the employer
19 went to check it and there was a problem with some sort of
20 reconciliation of your work status, the self-check is
21 designed to allow you individually to check, to go and say,
22 oh, there seems to be a problem with my Social Security

1 number; I'll get this resolved before I move to that new
2 job.

3 It has several privacy protections built within it
4 in terms of we have a third party identity provider that
5 will ask two to four questions based on your knowledge base
6 in terms of what street did you grow up on and so on, to try
7 to verify your identity.

8 Ms. McNABB: My SSA records?

9 MS. CALLAHAN: No. The third party identifier is
10 -- the third party ID provider is a commercial entity
11 that'll do it, and if you're able to answer that then it
12 will then go and do a ping off of SSA to see if there indeed
13 is the work eligibility.

14 The identity provider doesn't retain that
15 information at all. They also don't share that information
16 with E-Verify. They don't say, Joanne McNabb checked on
17 such-and-such day, and so on. They basically give a green
18 light to the individual.

19 So that will roll out, as I said, I think March 21
20 by E-Verify.

21 Ms. McNABB: And in a specific region, and how
22 will people be informed about it, and how will they do it?

1 MS. CALLAHAN: I am not the PR person for E-
2 Verify. Donald may know? I don't know if Donald's here
3 yet.

4 MS. PRESSMAN: It's in a trial in five states, of
5 which Arizona, Washington, D.C., Virginia -- it's going to
6 be posted Friday and there are going to be some
7 announcements from U.S. CIS on Friday. It's going to launch
8 on March 21.

9 Ms. McNABB: And would people be doing it online,
10 then?

11 MS. PRESSMAN: I believe March 21 is when it will
12 be. But it's only going to be available in certain states
13 at first.

14 MS. CALLAHAN: Yes, but it's an online
15 opportunity.

16 Ms. McNABB: It's online.

17 MS. CALLAHAN: Yes.

18 Ms. McNABB: Thank you.

19 CHAIRMAN PURCELL: Thank you.

20 So we have Annie, please.

21 MS. ANTON: First I'd like to commend you on your
22 amazing rate of handling all of those FOIA requests.

1 MS. CALLAHAN: Thank you. They've done a great
2 job.

3 MS. ANTON: That's really great.

4 I was curious, though, since there's such a
5 significant spike, increase this year, if we have any idea
6 what we can attribute that increase to?

7 MS. CALLAHAN: With regard to FOIAs, about 70
8 percent of FOIAs that the Department receives are actually
9 requests for immigration files, so primarily to U.S. CIS,
10 alien files, change in status and so on. At the end of --
11 basically the last 4 or 5 months of fiscal year 2010, U.S.
12 CIS received a 30 percent spike in FOIA requests.

13 Speculation on my part, maybe that because CIS got
14 the backlog down 2 years ago -- they did heroic work on
15 getting the backlog down and processed, I think personally
16 processed, over 100,000 FOIAs in FY 2009 -- people are like:
17 Oh, they're actually processing it; I'm not having a delay.

18 Related, there is of course the conversation about
19 comprehensive immigration reform and immigration in general,
20 so people may be seeking to get their records.

21 Interestingly, that spike in U.S. CIS FOIAs has
22 been pretty -- it's been pretty steady, but actually dropped

1 off a little bit last month in terms of looking at the
2 numbers each month.

3 MS. ANTON: Thank you.

4 MS. CALLAHAN: But it was pretty much a 30 percent
5 increase across the board for individual requests, kind of
6 Privacy Act requests, policy types of requests as well.

7 CHAIRMAN PURCELL: Thank you.

8 Ramon.

9 MR. BARQUIN: Mary Ellen, I have to ask because
10 you teased us by saying that --

11 MS. CALLAHAN: I don't tease, Ramon.

12 (Laughter.)

13 MR. BARQUIN: -- the data integrity train had
14 finally left the station.

15 MS. CALLAHAN: Oh, that's Eric. Eric's going to
16 talk to you about it.

17 MR. BARQUIN: Okay, fair enough.

18 (Laughter.)

19 MS. CALLAHAN: Good thing he's ready.

20 CHAIRMAN PURCELL: Fine.

21 Then Jim.

22 MR. HARPER: I wanted to just I guess endorse and

1 echo the question posed by our Chairman and bus driver,
2 Richard Purcell. The DNA dust-up that happened the other
3 week was maybe emblematic of maybe an institutional problem,
4 that a lot of things are going on at DHS, some of which have
5 obvious and serious privacy significance, and it's a matter
6 of personal embarrassment to me that I learned about it when
7 a reporter called, and it probably should be institutionally
8 embarrassing to the committee that we learned about it by
9 reading about it in the press.

10 I serve also on an occasional group at the
11 Homeland Security Institute, where these things are reviewed
12 quite well in advance, and it seems like maybe this
13 committee should be involved earlier in more things so that
14 things like this don't happen. I don't think that -- I
15 don't know that this particular program is a serious error
16 on the part of the committee to not have gotten a look at,
17 but it could be one of these things that is experimental
18 until we are presented with it as a fait accompli and asked,
19 perhaps asked, what we think of it.

20 So I wonder if you'd consider maybe some serious
21 changes in the approach so that we actually are ahead of the
22 ball, rather than behind the ball, on issues like this.

1 MS. CALLAHAN: We'll certainly take it under
2 advisement. Thank you.

3 CHAIRMAN PURCELL: Thank you. Thank you very
4 much, everybody.

5 Mary Ellen, thank you again for your time today.
6 I appreciate it. Thank you for all your comments.

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

8 CHAIRMAN PURCELL: We turn now to our next
9 speaker, who is Howard Schmidt. I have to say we're
10 privileged to have Howard here this morning. Howard is a
11 Special Assistant to President Obama and Cybersecurity
12 Coordinator for the federal government.

13 I can speak from experience that Howard has had a
14 long and distinguished career in defense, law enforcement,
15 corporate security, academia, and international relations.
16 I won't say for how long, but Howard and I served together
17 as the security and privacy officers of a major corporation
18 and I can only say that I enjoyed the professional
19 relationship enormously and am delighted to see in his
20 current position that Howard is responsible for coordinating
21 inter-agency cybersecurity policy development and
22 implementation and for coordinating the engagement with

1 federal, state, local, international, and private sector
2 cybersecurity partners.

3 I remind the audience once again, if there are
4 questions, we won't have time for those, but if you do have
5 questions of Mr. Schmidt please address them to Martha
6 Landesberg at privacycommittee@dhs.gov or in person here and
7 she'll take the questions and she'll forward them to Mr.
8 Schmidt for a response.

9 We're pleased to have Howard today to update us.
10 Howard, you're very welcome here.

11 UPDATE ON THE OBAMA ADMINISTRATION'S
12 CYBERSECURITY EFFORTS, BY HOWARD SCHMIDT

13 MR. SCHMIDT: Well, thank you very much, and I'm
14 very pleased to be here. Let me start with the apology for
15 missing the last time I was trying to make it over here, but
16 I think we all recognize, not only just in D.C., but any in
17 this business, anywhere in the world in this business, that
18 things come up at the last minute for some reason or
19 another, that are always a crisis. We have our share of
20 them.

21 Anyway, it's great to be here, and particularly
22 this week with the CDT dinner last night, the IAPP meeting,

1 and everybody sort of congregating here in D.C. to deal with
2 some of these important things that we're talking about.

3 I want to do a couple things today if I could.
4 Just, one, sort of update everybody on where we are on sort
5 of the continuum of the Cyberspace Policy Review,
6 particularly as it relates to some of the things the
7 committee's focused on, as well as to drill down a little
8 bit on the National Strategy for Trusted Identities in
9 Cyberspace, yet another "N" something or another, in this
10 case the "NSTIC," as we call it.

11 But before I get started with that, I'd like to
12 introduce Naomi Lefkovitz, who is our second official
13 privacy and civil liberties person in my office. When the
14 President created my office, a couple things were very
15 specific. One of them, create the office, create my
16 position. But the second thing was a very specific
17 directive, and that's we will have a dedicated director of
18 privacy and civil liberties who works in the office.

19 Naomi comes over from the Federal Trade
20 Commission, where she's been a senior attorney in the
21 Division of Privacy and Identity Protection. So I'm very,
22 very pleased that she was willing to come over and spend a

1 significant amount of time with us, helping us deal with
2 these issues specifically.

3 It was interesting because the nexus between the
4 work that I think you do and Naomi did was sort of the
5 confluence of the data security and identity theft
6 components of things, which we care about, but also the data
7 privacy protection. I think that's important to make sure
8 we look across the whole spectrum of what's going on across
9 the U.S. government, working with the great privacy officers
10 we have across the government organizations, departments,
11 and agencies.

12 A couple things that she's specifically working.
13 Of course, you'll be hearing this a lot: the NSTIC
14 implementation, ensuring that everything that we talk about
15 in that strategy has a privacy review in depth, that we're
16 acting on the things that we see that need to be implemented
17 relative to the strategy, and that has been a big thing that
18 we've been working on in the recent past.

19 But also ensure that we've got the privacy
20 oversight in the broad swath of U.S. government programs.
21 When we start looking at the coordinating role of the White
22 House, my role is kind of unique in many senses. One, it's

1 sort of a new office within the White House structure to
2 begin with, but also I'm dual-hatted within the national
3 security staff as well as the National Economic Council. So
4 as a result of that, we've got sort of a broad mandate to
5 look at the things across government in a coordinating role.

6 So clearly Naomi's role will be looking at this
7 piece across the U.S. government, ensuring that all the
8 great folks that we've got out there are not only looking at
9 the same issues, but looking at them so we're not being
10 redundant, we're making sure we're taking in all the various
11 components of privacy and civil liberties we deal with, but
12 also to make sure as we go through this government process
13 on cybersecurity that we don't look at it, well, there's a
14 tradeoff here and a tradeoff there.

15 I think that the Chairman probably has heard this
16 more times than he chooses, but we've held for a long time
17 that privacy and security are two sides of the same coin.
18 You can't have security without privacy. You can't have
19 privacy without security, and in many cases, whether it's
20 the data protection or it's the controls over how you manage
21 your own data, clearly there's a security component for it,
22 and we want to make sure that there's not some sort of a

1 tradeoff that we're doing, because clearly we can have both
2 and we need to have both of those things.

3 But anyway, so those are sort of the specific
4 efforts that Naomi is working on our behalf. Once again,
5 thank Naomi for her willingness to come over and spend a
6 good chunk of her life, not only in actual days, but in
7 White House days, which I think there's like a seven to one
8 ratio.

9 The next thing I want to sort of touch on is the
10 Cybersecurity Policy Review. We have had a number of
11 documents over the years relative to the government. I
12 think many of you were probably involved in the original
13 National Strategy to Secure Cyberspace in 2003, which by
14 many accounts -- that was one of the first instances where
15 we created the strategy about cybersecurity that had very
16 specific language in there about privacy. I can't think of
17 a time in the years that I spent, and very thankful that
18 Richard didn't bring out how many years, but I don't
19 remember anything that basically called it out specifically.

20 So that was sort of the first one.

21 The second one was the CNCI, the Comprehensive
22 National Cybersecurity Initiative. I think many of you --

1 and I thank many of you as well -- recognized that about a
2 year ago last month we released the unclassified version of
3 the CNCI, which many of us when we looked at that, when the
4 office was set up, it was like, why is this classified, when
5 we're particularly trying to ensure that we're being open
6 and transparent and all the things that the President has
7 asked us to do, not only by word, but also by specific
8 direction, that when we look at these things and how can we
9 ask our partners in the community to work with us on this if
10 we can't tell them what it is that we're looking to work on
11 together. So that was the next step.

12 The third thing is actually the Cyberspace Policy
13 Review. When the President came into office he said,
14 listen, we've got these sort of documents from the past; how
15 relevant are they? What are the things we need to look at?
16 Out of those, we identified some short-term goals to work
17 on. Two of them were the appointment of my position and
18 Naomi's position specifically, so those were done.

19 But I'm happy to say the vast majority of the rest
20 of them have also either completed or in near completion.
21 So when we start looking at some of these pieces of it, some
22 of the goals were: one, developing a national incident

1 response plan for cybersecurity. Once again, this was an
2 all-government effort, all-private sector effort, all of
3 academia. We had tremendous input, and we continue to mold
4 this, as witnessed by the Cyber Storm 3 exercise last year.
5 We had tremendous support from all quadrants, including our
6 international partners, not only to make sure that we can do
7 the things we need to do to recover from a cyber-related
8 incident, but do it in a manner that preserves our privacy
9 and civil liberties and not all of a sudden an incident
10 takes place and all that goes off to the side.

11 I'll use this term more than once. Richard
12 reminded me of it as well, and that's "privacy by design."
13 When you do an incident response plan, you have to have that
14 designed in there. The time to deal with these issues is
15 not in the midst of a crisis and start passing out business
16 cards and say, and how do you plan into this?

17 The other thing is the public awareness of cyber
18 threats and educating the public. We start looking at the
19 rich, robust capabilities that technology has given us in
20 many different fronts. We've benefited from a financial
21 perspective, from an entertainment perspective, from a
22 communications connectivity perspective. But clearly there

1 is bad actors out there. I think that's probably the
2 gentlest way of putting it.

3 But what happens is, when we start using these
4 technologies not everybody's aware of the bad actors out
5 there. It was interesting. Last night, doing some Facebook
6 stuff we were doing together, I started seeing things pop up
7 that, on the face look like, yeah, why wouldn't someone want
8 to do that? And the reality turns out it was a bad actor
9 that was affecting things that we enjoy and that we
10 socialize together on.

11 So making sure that we had a comprehensive program
12 in place. The mantra is "Stop, think, connect." DHS did a
13 tremendous job kicking this off with the private sector. We
14 did a bicoastal launch via web technology, of course, in
15 October, and really setting this up to broaden just more
16 than a bunch of government folks getting together and
17 sharing Powerpoints and saying, be careful, watch what you
18 do, update your systems, and all the things that have
19 somehow been the focus of prior awareness programs that we
20 have put out.

21 That is a living entity. It wasn't just October
22 is here, October is gone, move on. It continues. We have a

1 cyber PSA, public service announcement, contest, which I
2 think is just about to wrap up, led by Department of
3 Homeland Security, looking for the public to develop and
4 help us develop the messages, and out of that is a contest
5 and they'll be interacting directly and be highlighted by
6 the Department of Homeland Security through their web site
7 and other things.

8 So the awareness and education program is in full
9 bloom and it's one of the short-term things we looked at.
10 On that piece of it, there's the education piece, the
11 National Initiative for Cybersecurity Education, which is
12 sort of a cornerstone of this. So it's not only the
13 education and awareness for the public and the consumers and
14 end users, but also what are the career paths that we're
15 looking at? How do we wind up -- once again I'll say it --
16 having privacy by design built into the things that we're
17 looking at in the future? How do we create that workforce,
18 both in private sector and in the government, that says,
19 here's all the components of being more secure in cyber
20 space?

21 I think for those that come from the academic
22 realms in particular -- we have them on both sides of the

1 table over here -- you know it's not just about a computer
2 science course that says, here's how you do technology.
3 There's a lot of other components. There's the business,
4 there's the legal, there's the privacy component.

5 So the next generation of experts should have that
6 skill set built in. Those of us who have been around for a
7 long time, it's sort of almost by osmosis in some cases. We
8 found out we were doing something, there was another
9 component that needs to be built in, we really didn't take
10 into consideration as the careers were developing. So the
11 NICE program does that, and we're really moving forward on
12 that.

13 The Department of Education is a part of it. NIST
14 is a part of it. All the right government folks are there,
15 plus our private sector partners as well.

16 The other couple things that I think are important
17 -- in the next couple months, as far as national strategy,
18 as I mentioned, the NSTIC, but we'll also be releasing an
19 international strategy. Mary Ellen was talking about some
20 of the international components, the things we're doing.

21 As we live in cyber space, it's not as if we have
22 some geographical boundary that says, here's the only thing

1 that we can deal with. So having an international strategy
2 which embodies the principles of privacy and freedom of
3 speech, not just a footnote, but embodies that in a national
4 and international strategy, so not only do we say this is a
5 core value of ours, but also to make sure we're clear with
6 our international partners that the expectation is that
7 that'll be a part of their philosophy as well. We've seen
8 tremendous -- I don't think anybody in this room is not
9 aware of what's happened the past few weeks, to really show
10 the power of the technology and what it's been able to do
11 for freedoms and democracies, and we hope that that
12 continues.

13 So trying to focus now a little bit more
14 specifically on the NSTIC. It's coming up real soon. I
15 think, running the risk of giving a specific date, which is
16 always scary because you know when you do that there's
17 something that comes up that changes that, but it will be
18 released very soon. Probably many of you are aware that
19 Secretary Locke and I did the announcement on the creation
20 of the national program office within the Department of
21 Commerce with NIST a couple months back out at Stanford.

22 I think that was another thing that I think was

1 very clear. By housing this within the Department of
2 Commerce, it really sends a clear message that this is an
3 environment where we have to have commercial understanding,
4 we have to have the privacy components, we have to have the
5 telecommunications component of that, working with the rest
6 of the government, working with the rest of the private
7 sector.

8 But the question we get all the time, well, why is
9 the government involved in this? The very specific answer
10 is the fact that this is a catalyst. We've been talking
11 about this for a long time. In my own less than eloquent
12 way, I say we've been admiring this problem for a number of
13 years. How do we wind up getting past the world where we
14 have privacy issues, we have cyber crime issues, we have
15 identity theft, credit card frauds, based oftentimes on the
16 fact that we're still living in a society that has passwords
17 and user IDs as the main way to authenticate anything?

18 So trying to move around that and saying, how do
19 we get beyond that, how do we have an authentication
20 mechanism out there that gives us, both as an individual
21 consumer, as well as businesses, to make sure that I'm
22 dealing with the people that I think I'm dealing with, with

1 some level of credibility in doing that?

2 When we start looking at the online services -- to
3 give you an example I gave a little while ago, we were
4 sitting there and saying, I don't know who that really is on
5 the other end out there. In some cases, I may not care.
6 But making sure that we have a mechanism, if we care there's
7 a mechanism to do it, that's led by the private sector.

8 The other piece we'll be looking at when we look
9 at the policy development and leveraging of the privacy-
10 enhancing technologies that we're looking to do through the
11 NSTIC, we're looking to have that what we refer to as the
12 Identity Ecosystem founded and grounded in the Fair
13 Information Practice Principles or the FIPPS, to achieve our
14 objectives.

15 Going back to the phrase again, privacy by design.
16 You know, when we start looking, when the principles were
17 first brought out, we were already way down that path of how
18 we interact online, what are sort of the principles. We're
19 trying to retrofit them in many cases, whether it's through
20 browser privacy settings that didn't quite work from the
21 very outset. But this gives us an opportunity to design
22 that ecosystem, not based on something we understood 3, 5

1 years ago, but what are the things we're going to need for
2 the future.

3 In that ground, very specifically it's saying this
4 is our opportunity to say, here are the principles that we
5 need to apply, here's the technologies, here's the controls
6 we needed to put in place to make sure these are implemented
7 that I don't need to go into a position where I've got to
8 check 14 different boxes, oh, yeah, by the way, and a month
9 later go back and see if those boxes have changed on me.
10 That's not the way we're looking to design that ecosystem.

11 When we start looking at the evolution of the
12 technology, I think we all recognize that it was an
13 opportunist type thing. Great technology, let's go deploy
14 it here, and a lot of the things we look at from security
15 and privacy were once again the bolt-on aftermath thing, and
16 here's our opportunity to design the system right, including
17 looking for an environment where things don't work right.

18 How do we wind up countering the bad actors that
19 invariably will try to come into this space and my idea --
20 not me, but the bad guys' idea -- of providing an identity
21 service provider to collect everything I can on you and run
22 for the hills? We have to have a mechanism in place to

1 protect against that.

2 So there's going to be a lot of pieces to this and
3 it's not going to be an overnight thing. But here's our
4 opportunity to really change the game the way we play this.

5 The other, the third principle which is key, it's
6 opt in and optional. When we start seeing what's happened
7 over the past month, that has really reinforced, if there
8 was any doubt in anybody's mind, the ability we need to
9 maintain to keep that anonymity in the things that we do.
10 We don't want to see positions where people are arrested,
11 persecuted, or in cases, in some cases, maimed or killed,
12 because they're expressing the things that they believe in.

13 We need to make sure that vehicle still exists for
14 people. So while we're doing trusted identities for those
15 transactions, we need trusted identities, we have to
16 preserve the ability to operate with a level of anonymity in
17 the system we have now, so people can protect that; and also
18 make sure that as the ecosystem builds out one of the things
19 that many of us have talked about is, yeah, well, how about
20 we build something and it becomes sort of the de facto
21 standard, that at some point that's going to edge us out of
22 the ability to do things that give us the ability to do

1 anonymous freedom of speech. The thing is, once again, as
2 we build this we need to preserve that. We need to make
3 sure the controls are in place, where 10 years down the road
4 we're not looking back and saying, God, I wish I would have
5 thought about that and built in a control to make sure
6 somebody doesn't erode the things that we care about today.

7 Then the last principle is giving choices. I, as
8 many of you, interact with a wide range of people, people
9 that say, hey, I have this little device, I flip it up and I
10 talk on it, that's all I need it to do, to others that,
11 basically, most of us have three or four different types of
12 devices we use for communications, we have great technical
13 skills.

14 But the idea of saying this one piece of
15 technology is going to be the only thing that you need is
16 not what we're looking for, whether it's smartcards, one-
17 time passwords in mobile devices, little necklace chains
18 that we carry around, and I don't know what other technology
19 may even be out there. But give people a choice of what
20 they want to use, if they want to use something, but also
21 preserve the ability to have multiple choices, because the
22 fact that I'm going to get a free dozen eggs with a gallon

1 of milk that I buy -- yeah, I probably would want to do
2 that. Most of us would. But that doesn't mean I have to
3 sell everything in my house from a privacy perspective in
4 order to get that.

5 So what is the mechanism I do that? Whether it's
6 something that merchants get together and say, here's your
7 little promotional loyalty thing that you can use and it's
8 federated amongst a dozen different things, that if
9 compromised, what happens, I have to go ask for another one
10 to get a new set, a new dozen eggs in there.

11 But we have to think about these things. We also
12 have to understand when we start looking at these choices,
13 what are the choices that are going to affect the people
14 that just don't know any better? Because one of the things
15 we've looked at -- and say I'll use PIN and chip technology
16 as an example. Man in the middle type attacks, the ability
17 to actually get physical access to a card and do something
18 to it. We know that has happened. Here's our opportunity
19 to make sure we take that into account as we're building the
20 next generation of technology, whatever it may be, to help
21 preserve these things.

22 A couple other things that are caveats that we

1 call out specifically in the strategy. Number one, we have
2 to make sure we don't create this sort of uber-database of
3 information, which not only becomes a potential attack
4 vector for hackers and criminals and anybody who's looking
5 to do things with it, including commercial interests that
6 may say, yeah, here's my opportunity to really market where
7 I didn't have an opportunity before, to ensure that that is
8 not created either by the government or the private sector.

9 So as we move forward on these things, a lot of
10 these principles that we talk about, we have to embody those
11 in strong policy and protect those.

12 Then when we look at the ecosystem itself, that's
13 exactly what it is. We have to make sure all these pieces
14 fit together, and if indeed, if I've got a computer system
15 that is compromised with a keystroke logger and my mechanism
16 of having a trusted identity to do financial transactions or
17 ecommerce, that it's not going to be affected by something
18 that's not working right on the computer system or working
19 in a degraded environment, so to speak.

20 The other thing, and it's amazing --
21 notwithstanding Secretary Locke being very clear, I was very
22 clear, and many of the folks that really know this thing

1 have been very clear on, this is not a national ID card.
2 It's not looking to be a national ID card. As a matter of
3 fact, many of us would rail against the fact of anybody
4 trying to make it into that.

5 These give us new opportunities that we've not had
6 before. So by having the users have the choice of saying, I
7 want one for this side of my life, I want one for this side,
8 or I don't want any at all, that's what it's about, but also
9 finding some of the things that we can leverage.

10 The example that they use ever since we first
11 started talking about this, and it still happens, which is
12 surprising, I'll walk in, I'm traveling somewhere, I stop
13 and ask for a beverage that requires proof of your age over
14 21, which is generally not tomato juice. And what's the
15 most common form of identification, is driver's license. It
16 just doesn't say "Over 21" on there. It has a lot of
17 personal information that we don't need to present.

18 You start thinking of the mechanism and start
19 thinking of the things that we really care about. Buying a
20 device, particularly one that has a recurring monthly
21 charge, we have to prove that we're creditworthy, we have to
22 do a Social Security number, we have to have date of birth.

1 That may be valid for that transaction. I'm not discounting
2 the fact that we want to make sure that we're not having
3 businesses toppling over through fraud and things.

4 But the fact that they need that for more than
5 about 3 milliseconds is something that we can help build in
6 this infrastructure. So not looking to create this national
7 ID that says, here's what we've got and here's what
8 everybody must comply with.

9 The other thing is that we're very clear on is,
10 there's no government mandate that people need to do any of
11 this. We're looking for the private sector to do this, for
12 the innovators and the entrepreneurs to come out to work
13 with many of us in the privacy and security community and
14 say: How is this really going to work? Some people may say
15 this is a great business opportunity, and we've all
16 benefited from the business opportunities that the
17 technology has presented to us.

18 So this may be a great opportunity to leapfrog
19 some of the sort of slow path that we're on in dealing with
20 some of these things.

21 The other thing is, when we start looking at the
22 people that are victimized over the past 10, 15 years, and

1 you go to multitude web sites that show the data breaches
2 that have resulted in either direct impact on individuals or
3 the potential. As we've talked about many times, the fact
4 that there was a data breach 2 years ago and we haven't seen
5 anything happen in our life doesn't mean 5 years down the
6 road, if we're depending on that same identification
7 mechanism -- Social security numbers, date of birth, all
8 these other things -- that somebody just can't revive that
9 old database that they stole and say, okay, here we go.

10 So we can develop a system in the mean time that
11 sort of discounts that, that minimizes the likelihood of
12 something like that that takes place.

13 So the bottom line is there's a lot of moving
14 parts in this that I think collectively as a community we
15 can really move forward on. I don't expect it to happen
16 overnight. I don't expect it to be 100 percent of anything.
17 But I think now we've come far enough down the path that
18 we've got an opportunity to really build it the right way
19 moving forward.

20 The closing note on that is, privacy by design in
21 all the things we're doing moving forward.

22 So in conclusion, as I mentioned, the Department

1 of Commerce will be hosting the National Program Office.
2 I'm very pleased that they hired Jeremy Grant to head that
3 office. If you don't know Jeremy, he's got a great resume,
4 he's got great understanding of the issues we're dealing
5 with here, and he's a great one, and I'm very happy that
6 they picked him to lead that office.

7 NIST and the folks over there are going to be part
8 of making, working this forward, bringing the right people
9 together, looking for the right pilots, looking for a way to
10 move this forward. I'm really, quite honestly, excited with
11 the fact that we're finally doing something about it and not
12 just admiring a problem any more.

13 So with that, Mr. Chairman, thank you for the
14 opportunity to sort of give you the update and I very much
15 thank you all for the work that you're doing, because I know
16 this is more than just a meeting and then everybody goes on
17 with their real lives. This is part of the life that we
18 have. So thank you for all that.

19 CHAIRMAN PURCELL: Howard, thank you very much for
20 those comments. That's very helpful.

21 One thing I'm concerned about is barriers to
22 entry. I totally support the Commerce Department drive.

1 It's a catalyst, it's a market-creating opportunity to a
2 great degree. But of course, barriers to entry in this
3 market could be nominally high. Lowering those barriers to
4 entry has the converse problem of allowing bad actors to
5 perhaps get involved and use it as a platform for their
6 activities as well.

7 So how are you going to -- is there a plan or is
8 there a discussion going on about where the sweet spot is to
9 make it available by lowering the barriers to entry so not
10 just the largest players on the planet are able to play, but
11 at the same time making provisions so that script kiddies
12 can't get involved and either do it poorly or do it for
13 nefarious purposes?

14 MR. SCHMIDT: Part of the strategy is getting the
15 smart people together to figure out where that balance is,
16 because when we were putting the office together, I
17 mentioned earlier, the idea is that there will be people out
18 there that say, hey, come get my great ID, you'll do all
19 this stuff, collect everything they can on you, and they're
20 gone and you've got a problem.

21 So figuring out what is the right vetting process
22 to go through this, to make sure that those who are going to

1 be issuing credentials are going to be in a trusted
2 environment, they're going to require somebody to give up
3 some PII to do it, that we try to keep them out of the
4 market. Don't know the details, which is why we've got the
5 program office set up. That's one of the things we've got
6 to check off, is how do we minimize the risk that somebody
7 could be successful in doing the bad actor type things, and
8 if indeed somebody winds up slipping through -- and I'll
9 use, for example, the insider threat that we've all talked
10 about for a number of years.

11 I don't know anyone that's ever hired anybody that
12 says: I'm going to hire you under the premise that I know
13 some time in the near future you're going to create --
14 you're going to start committing embezzlement in my company.
15 There's always an opportunity for somebody to start out good
16 and go bad, for whatever reason. The ability to turn that
17 off and the ability to -- an example that I like using, and
18 I hope it's not only feasible, but it's practical -- to say,
19 okay, I'm doing business with you, but I have the ability
20 under my control to turn that off and to make sure that
21 everything you've got on me I have the ability to self-
22 destruct it, without you having any ability to block it or

1 stop it.

2 It's a nice way of looking at it and I think if we
3 look at the right technology, look at the right business
4 processes, we'll actually have the ability to commit
5 something like that.

6 CHAIRMAN PURCELL: Thank you.

7 MR. SCHMIDT: Thank you.

8 CHAIRMAN PURCELL: Jim.

9 MR. HARPER: Thank you, Mr. Chairman.

10 Thank you, Mr. Schmidt, for being here. I
11 appreciate your comments. I've been particularly interested
12 in NSTIC and gotten a lot of calls and questions about NSTIC
13 and I've been reassuring a lot of folks who are even more
14 paranoid than I am. I do think that the intention of the
15 program is good, and you've stated well your intentions for
16 it.

17 As you know well, the devil is in the details. I
18 was thinking back to 8 or 9 years ago I reviewed with others
19 a smart roadways system, and at the sort of end of the
20 session they said: Okay, privacy is all protected because
21 the government has all the encryption keys. You get the
22 joke, I think.

1 MR. SCHMIDT: I do, yes. Trust me.

2 (Laughter.)

3 MR. HARPER: So it's an exercise in imagination to
4 express concerns like this, but I worry, and I don't know
5 how it might play out. But the catalyzing role that this
6 plays could, for example, result in the community of
7 identity providers, the industry, saying, you know, this all
8 would really work if the government were just to provide
9 everybody an X-509 certificate. Then, despite everything
10 you've tried to do in terms of protecting against that kind
11 of centralized uniform ID process, you do have one that is
12 centralized, uniform, and likely would result in a national
13 ID, if not be one.

14 So give me just a little bit more. What in the
15 report provides me that assurance that this isn't a catalyst
16 for political consensus around that kind of system? What
17 are the real concrete pieces in there that say no way, no
18 way; this has to be a distributed, bottom-up environment?

19 MR. SCHMIDT: Pretty much that language. It's
20 part of the strategy. Once again, it's interesting because
21 the discussions I've had with people is what this could
22 morph into in the future, what could it evolve into. I wish

1 I could sit here with some level of certainty that said, 10
2 years from now some future government agency may say, hey,
3 we've got this and we're going to move forward on it. And
4 the only thing I can say, because I probably won't be around
5 and some of us may not be around, is to make sure it's
6 important as we develop this system that we put those checks
7 and balances in place.

8 I don't know what they'll look like, whether
9 they're legislatively, whether they're policies, whether
10 they're technologies. But basically it says this will not
11 happen on our watch. I can't speak for what may happen in
12 the future, but we sure will -- well, you know yourself, for
13 those of us who maybe have a little bit of paranoia, we're
14 going to keep a close eye on this thing as it develops, as
15 it develops to benefit us, not to where somebody can in the
16 future change it to benefit them.

17 CHAIRMAN PURCELL: Neville.

18 MR. PATTINSON: Always good to follow Mr. Harper.

19 Mr. Schmidt, thank you very much for coming today.
20 I've been following NSTIC since March last year and
21 thoroughly applaud the privacy by design that's been taken
22 into the development of the draft strategy as it stands. I

1 look forward to seeing that come out in short course.

2 Part of this is really how it's all going to work.
3 It's a great ecosystem, great vision. Obviously, I think
4 there's a whole area of governance that needs to be
5 addressed quite quickly with NSTIC. There's a lot of
6 stakeholders potentially that need to be involved, from
7 private industry, from academia, etcetera, and certainly the
8 government needs to have involvement in this.

9 So what role do you see the National Program
10 Office -- and certainly, DHS, you have a terrific resource
11 here in the Privacy Office -- in assisting with that
12 governance? Obviously, there needs to be the forum that
13 needs to be created. But to what extent are they going to
14 be involved? Is it as observer, is it funder? I would like
15 to know that kind of understanding in your mind today, as
16 well as then if you have any plans for government adoption
17 of the results, because that will create industry's interest
18 and everything to drive the adoption from consumers,
19 etcetera, for uses, for potentially signing tax forms in the
20 future? Let's have a real government application that could
21 also assist not just the private sector.

22 MR. SCHMIDT: That's a wonderful example, and I'll

1 start with that question and hope I can remember what the
2 first one is. If not, I'll ask you. But as far as the
3 government application, we have an interest in this as well,
4 because what happens is when you start looking at the
5 interaction between the government and citizens on just the
6 normal, day to day business -- you used the tax thing. I
7 think of my travel needs and going through Customs and all
8 those things that I do currently.

9 What we want to do is, whatever gets developed out
10 there, that we have the ability to benefit as well as the
11 customer. So as we develop this ecosystem, one of the
12 things I'm told multiple times is the reason you can't do
13 more with some of the services that the government provides
14 without physically going in the office is because we can't
15 do that strong authentication that we really know it's you,
16 that it's not somebody else doing something else.

17 So we have a tremendous appetite for this and
18 that's one of the things that the program office is looking
19 at, is where are the applications the government can say,
20 okay, if I decide to go to my local grocery store and they
21 have an ID schema that I'm comfortable with and I buy, that
22 has some level of assurance, they do in-person proofing or

1 something like that -- I'm getting out there a stretch on
2 the grocery stores, but you get the point -- and the
3 government says, I recognize that will work to interact with
4 us for these things, we should be setting that up.

5 That's what the program office is looking to do,
6 what are the applications. The one you mentioned, taxes, is
7 probably going to be pretty high up on the scale.

8 MR. PATTINSON: On the question of governance and
9 the National Program Office and the Privacy Office here and
10 that body that's going to need to be created?

11 MR. SCHMIDT: As it stands now, it calls for a
12 governance model. The governance model has got to be
13 determined by the stakeholders involved there. So we'll
14 have the private sector folks, we'll have government folks
15 that will be involved. The standards folks at NIST
16 particularly are going to be the key drivers of this, as to
17 how do we make this all come together, not only from a
18 technology perspective, but governance as well.

19 The governance includes things we have mentioned
20 earlier, like how do you get rid of the bad actors, how do
21 you minimize the likelihood they get in there, but also how
22 do you support the ones that are really doing the right

1 things for us.

2 MR. PATTINSON: Thank you.

3 MR. SCHMIDT: Thank you.

4 CHAIRMAN PURCELL: Thanks.

5 David, please.

6 MR. DAVID HOFFMAN: Howard, thank you very much
7 for coming here. I appreciate it.

8 I've got a two-part question. The Cyberspace
9 Policy Review noted this duality, this essential duality of
10 what we need to accomplish, of really needing to harden our
11 systems and networks to make sure that we protect the
12 infrastructure and protect the data that's carried on or
13 within the infrastructure, but also then being able to
14 provide a mechanism for law enforcement to be able to get
15 access to data when it needs to, to investigate crime and to
16 protect against terrorism.

17 So we're not the only country struggling with
18 that, and I think since the review's come out it's become
19 even more profound, that many other countries are really
20 looking at this. So my questions are how are we -- how is
21 the administration looking to role model what we would want
22 other countries to adopt within that duality? Then number

1 two, what are we looking at -- once again following up on
2 Neville's comment -- around oversight in that area, and
3 specifically if it's possible at all to comment on, will we
4 see any activity on the privacy and civil liberties
5 oversight board?

6 MR. SCHMIDT: I'm glad I didn't bet money on
7 whether or not I was going to get a question about the PCLOB
8 or not.

9 (Laughter.)

10 Specifically on the international, that's one of
11 the things on the international strategy that's soon to be
12 released, is sort of what our expectation is from other
13 countries, because you're correct. And none of us want to
14 be the victim of the next terrorist attack. None of us want
15 to have our children victims of pedophiles and all these
16 other things, which are legitimate national security and law
17 enforcement activities that are impacted by the better
18 security we do in technology.

19 But I think that the fundamental premise is we're
20 not going to undermine security as a facilitator of opening
21 some other doors that normally would not be answered. We
22 went through this years ago, as we all know, on the clipper

1 chip and the crypto export issues, and I think we've learned
2 from that in many cases that security really is important to
3 do our data protection, to make our networks and our
4 infrastructure more resilient.

5 We also have that legal mechanism in place, and
6 that's one of the things that's a struggle right now on how
7 do you wind up preserving the security and the resiliency
8 that we want, but also make sure that we're not shuttling
9 the next group of terrorists into the country because
10 technology is so good they can hide behind it.

11 It will never go away as a tension. In my early
12 days in law enforcement, we dealt with it. But we have to
13 have the smart people thinking of those individual things as
14 technology changes.

15 The international strategy really lays that out,
16 that there is the things that we expect people to do to keep
17 their systems up and running and less vulnerable and
18 protecting the data, but also there's a judicial process
19 that we go through internationally, which is an imbalance.
20 We start looking at some of the basic tenets of the Budapest
21 agreement, the Council of Europe Cyber Crime Convention. I
22 think last count there were 30 some odd countries that had

1 either acceded to it or ratified out of 150-some. There is
2 a mechanism to deal with some of these things and it's not
3 at the expense of less security so we can do better
4 oversight and surveillance.

5 The other point was about the oversight.

6 MR. DAVID HOFFMAN: PCLOB.

7 MR. SCHMIDT: PCLOB, yes. Hoping you forgot that.

8 It's in progress. You know, we've got two
9 wonderful appointees thus far, and I think collectively as a
10 community in the privacy and security communities we're very
11 happy with those. Just the mechanism of all the appointees
12 and all the vetting all the things that go on and a
13 relatively small staff within the White House is more the
14 mechanics moreso than the desire.

15 MR. DAVID HOFFMAN: So we can be hopeful.

16 MR. SCHMIDT: And I have someone sitting directly
17 behind me who's been very helpful in making sure that I get
18 those phone calls: Where are we on this? We really need to
19 move this forward?

20 MR. DAVID HOFFMAN: Thank you, Howard.

21 MR. SCHMIDT: Thank you.

22 CHAIRMAN PURCELL: At some of our prodding, I

1 would say.

2 MR. SCHMIDT: Yes.

3 CHAIRMAN PURCELL: Lisa, please.

4 MS. SOTTO: Thank you.

5 Thanks so much, Mr. Schmidt, for joining us. You
6 have a formidable job.

7 I certainly understand that privacy is not first
8 on your list. You have a huge job to tackle and you've got
9 two, three, four, five, and six behind. Cybersecurity and
10 privacy is just one of the long list. So I very much
11 appreciate that privacy is not something that you do only in
12 putting out fires, but in fact you're thinking about privacy
13 as part of the broader framework, which is really
14 commendable.

15 My question really builds on David's. When you're
16 dealing in a borderless world, as you are, how do you rise
17 above the global cacophony of data protection laws? Do you
18 operate sort of at a different level that really is at a
19 30,000-foot level, so that you are rising above those tall
20 buildings that are obstacles otherwise in the international
21 framework?

22 MR. SCHMIDT: And thank you for the question. A

1 couple things. One, my job's not as difficult as it may be
2 made out to be, and that's because it's federated with all
3 of us in this room and many other people out there. It's
4 one of the really gratifying things, is this is not
5 depending upon a person. It's depending upon, once again,
6 that ecosystem.

7 Relative to sort of the data privacy issues, in
8 any conversation that we have either bilaterally or
9 multilaterally with our partners, once again at a fairly
10 senior level, this is part of the discussion. So it's not
11 here's the four or five priorities and here is privacy.
12 Here's the things we talk about on an equal plane relative
13 to security and privacy.

14 Even recent meetings that I've had with other
15 countries, where one may say, well, gee, that's kind of odd,
16 they may not be on the same wavelength with others on data
17 protection and privacy and freedom of speech, it doesn't
18 make any difference whether they are. They hear about it
19 from us and they hear from us the expectation is we're going
20 to be at that level. They may not be overnight, but our
21 expectation is we're going to be there.

22 So it's an interesting dialogue, and looking at

1 all the different ways that it's implemented around the
2 world and, by the way, also within the United States itself.
3 We have 45 different data protection and data breach
4 notification laws here we're working on. It's not something
5 that's lost on us, but we have that discussion every time we
6 have a discussion with somebody from an international basis.

7 And that's, by the way -- one other quick point --
8 it's informed by a lot of the stuff that you are doing, the
9 ISPAB is doing over at Commerce and NIST, and a lot of the
10 groups that really think about this all the time.

11 Thank you.

12 CHAIRMAN PURCELL: Recognizing that we're running
13 short on time, Ramone.

14 MR. BARQUIN: Very quick.

15 CHAIRMAN PURCELL: That means hurry up.

16 MR. BARQUIN: I'll hurry up then.

17 You are very much at the intersection within the
18 government of these three communities, the civilian
19 agencies, Homeland Security, and of course intelligence and
20 the defense folks. With the imagery of cybersecurity
21 quickly evolving into cyber war, the 800-pound guerrilla
22 amongst those communities really does have the ways and

1 means. How are you dealing with that so that privacy in
2 particular and data integrity don't just die stillborn?

3 MR. SCHMIDT: Well, first, when you talk about the
4 defense community versus the civilian government versus the
5 private sector, I think we all recognize the Department of
6 Defense has been long dealing with these issues before
7 anybody else, and recognizing the threats out there, the
8 vulnerabilities that we have and ways to mitigate those.
9 They have some of the best teams out there. I've said many
10 times, General Alexander when he was working that issue,
11 when he started dealing with these things, it was sort of
12 the first time I saw someone from a technology background
13 raise that level, fully recognizing that there are some
14 boundaries that they have to work with.

15 As we move forward, looking at the role of
16 Department of Homeland Security, civilian government's
17 relationship with the private sector, Department of Defense
18 not only protecting their networks, but looking at sort of
19 the external threats and how do we keep the U.S. from
20 becoming victims of somebody else because of nation-state or
21 military actions and the authorities that are associated
22 with that is why we put together the Joint Program Office

1 with the Department of Homeland Security.

2 Also recognizing that as the scenarios change in
3 the future -- we had a discussion this morning about an
4 exercise -- and how what looks like a civil cyber event
5 could evolve into something more dramatic, and where is that
6 handoff, indeed if there is a handoff. I think the bottom
7 line is, using terminology such as "cyber war" is
8 problematic to begin with. I know people have heard me talk
9 about this before. It's a terrible metaphor. I think it's
10 a situation we need to recognize what's going on out there.
11 We have economic espionage, we have identity theft, we have
12 credit card fraud. We have to develop norms in cyber space
13 and everything else.

14 But the bottom line is we recognize there are
15 boundaries, and making sure that no one takes that
16 responsibility lightly.

17 To the issue of using the war analogy in anything,
18 this is not something that people would have to decide
19 lightly. The same thing applies, and probably even more so,
20 in cyber space because you don't have a geographical
21 boundary that says, I can go in there and cordon this off
22 and make sure that the activities don't go beyond that. In

1 cyber space we're connected all over the place.

2 So working through the inter-agency process,
3 working, making sure with the privacy officers and everybody
4 involved in this thing, we're in a much better place now I
5 think than we were even 2 years ago, making sure that things
6 don't get off track as far as not only protecting security,
7 but also privacy as well.

8 CHAIRMAN PURCELL: Thank you.

9 Howard, please.

10 MR. BEALES: Thanks.

11 I was interested in your response to Neville's
12 question about the government as user of authentication
13 systems. I was wondering what the vision is of how the
14 government would go about deciding whose authentication
15 systems qualify. Part of what provokes the question is, we
16 have in some ways a similar model in the financial sector on
17 the nationally recognized rating organizations, that was
18 supposed to have competing views of what really is the risk,
19 another difficult question to assess. We ended up with
20 four. They ended up all thinking mortgage-backed securities
21 were wonderful things, and we know what came next.

22 So I'm wondering what's the vision of how the

1 government goes about what is a fairly difficult task of
2 figuring out whose standards are acceptable and how can we
3 evaluate that?

4 MR. SCHMIDT: Well, I think, number one, when we
5 start looking at the role of NIST as a standards body
6 working with the people in the private sector, and as well
7 as the government customers, number one, what is sort of the
8 standards from the technology? Then you add onto that the
9 governance piece of it, and then what indeed, what is the
10 right rating system that's going to be developed basically
11 that says, okay, for me to do less than \$100 transactions on
12 an auction site this is the level I need, the level of trust
13 I need in my provider to do this thing; and developing that
14 system with as much insight as we've got.

15 Once again, I have to heavily caveat that we don't
16 expect anything to be perfect. But what we expect to have
17 happen is the fact that the questions like you have and the
18 experience we've had in the past, we're saying, yes, we
19 thought this was really good and it wasn't, how can we avoid
20 that again? The devil's in the details and I think we all
21 know that.

22 That's why once the Program Office gets stood up,

1 once the strategy is out, the real work comes. But there's
2 got to be some sort of a rating system that's recognizable
3 without me having to do 20 hours worth of research to say,
4 yes, that's a good company or that's not a bad company to
5 trust my own PII with. That's the system we've got to build
6 on top of the technology itself.

7 CHAIRMAN PURCELL: Dan, you have the next, but
8 I'll reserve the last word.

9 MR. CAPRIO: Thanks for being with us, Howard.

10 MR. SCHMIDT: My pleasure, Dan.

11 MR. CAPRIO: We much appreciate it.

12 We've come a long way since 2003 and that first
13 national strategy. So just a quick question about timing.
14 You mentioned the international report. Can you give us
15 some sense or ballpark of when we can expect that?

16 MR. SCHMIDT: Yes.

17 (Laughter.)

18 MR. SCHMIDT: Soon.

19 MR. CAPRIO: Fair enough.

20 MR. SCHMIDT: Yes. And once again, that's the
21 tough part about being in this position, is the minute you
22 say within X amount of days or X amount of weeks, something

1 happens that changes it. But it will be soon.

2 MR. CAPRIO: So NSTIC is very soon, international
3 report is soon?

4 MR. SCHMIDT: Very soon and very soon.

5 MR. CAPRIO: Okay. Thanks.

6 MR. SCHMIDT: We've been really concentrating on
7 getting these things done.

8 MR. CAPRIO: Good. Thank you.

9 MR. SCHMIDT: Thank you.

10 CHAIRMAN PURCELL: Howard, I want to just say a
11 few words, probably mostly in thanks for being one of the
12 pioneer security individuals who recognizes that civil
13 liberties and civil rights, the privacy programs that have
14 been developed, are absolutely equal to and partnered with
15 all security programs. It's something of a commonplace
16 expression today. 15 years ago when you and I were doing
17 it, it was anything but. So I want to commend you for that
18 and thank you for that, and encourage further collaboration
19 between the committee and your office and further
20 communication.

21 With that, I'd like to invite Mary Ellen to say a
22 few words as well.

1 MS. CALLAHAN: I'm sneaking up on you. I'm
2 sneaking up on you.

3 Howard, I wanted to thank you very much for
4 joining us today. I echo all the comments today. You
5 talked about privacy and security being two sides of the
6 same coin. Well, I wanted to share with you the Privacy
7 Office coin, so you make sure you at least have privacy on
8 one side of the coin.

9 Thank you very much.

10 (Applause.)

11 MR. SCHMIDT: Richard, thanks for those comments.
12 I guess in short is the fact that there's a mentorship I had
13 with many of the people in this room over the years that
14 have really made this two sides of the same coin and
15 informed a lot of the things that we've been doing, because
16 without the leadership and mentorship we have in this room
17 and other places outside that says, here, think about this
18 too -- it really made a difference.

19 So thank you all for what you're doing and thank
20 you, Richard, for the kind words.

21 CHAIRMAN PURCELL: Always a pleasure. Thank you.
22 Thank you very much, Howard.

1 (Applause.)

2 CHAIRMAN PURCELL: We're going to take a break for
3 a short period. We're a little behind schedule, so we will
4 reconvene at 2:50. 2:50, please.

5 (Recess from 2:38 p.m. to 2:55 p.m.)

6 CHAIRMAN PURCELL: I'd like to begin our final
7 session for the afternoon. Again, welcome back and please
8 remember to silence your cellphones. I'm sure people did
9 updates and checked on status, but it would be most polite
10 if those were stowed and silenced for the remainder of the
11 afternoon.

12 Also, I want to again remind the members of the
13 public that the Committee will be delighted to have you
14 address questions or comments to us later this afternoon.
15 There's still time to sign up at the table outside the room
16 and we encourage you to do so, please.

17 I'd like to now introduce our next speaker, Donald
18 Hawkins. Donald, welcome. Donald's the Chief Privacy
19 Officer for the Department of Homeland Security's U.S.
20 Citizenship and Immigration Component, USCIS. In that
21 capacity, Mr. Hawkins directs efforts to ensure that the
22 USCIS adheres to federal privacy laws, regulations, and DHS

1 policies and practices.

2 His office is charged to sustain privacy
3 protections and the transparency of his component operations
4 while supporting both the Department and his component
5 mission. Prior to joining USCIS, Donald held positions in
6 the U.S. Secret Service, the Department of Justice, the
7 Office of Management and Budget, and served in the Air Force
8 from 1980 to 2003.

9 We look forward to Mr. Hawkins' brief on the
10 USCIS's implementation of privacy policies for his component
11 and consistent with the Department. Mr. Hawkins, welcome.
12 Please proceed.

13 UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES
14 IMPLEMENTATION OF DHS PRIVACY POLICY,
15 BY DONALD K. HAWKINS

16 MR. HAWKINS: Good afternoon, Committee. I'd like
17 to thank you for the opportunity to speak with you today. I
18 think the last time I spoke with the group was in 2007 in
19 Vegas. Without further ado, I'm going to jump right into
20 it.

21 CHAIRMAN PURCELL: That's fine. We'll leave it
22 there.

1 MR. HAWKINS: Okay.

2 (Laughter.)

3 MS. CALLAHAN: It is a privacy committee.

4 (Laughter.)

5 MR. HAWKINS: First of all, I want to cover a
6 little bit about what USCIS does as a component, talk a
7 little bit about the records that we collect and maintain
8 consistent with our mission.

9 USCIS is the world's largest immigration service
10 and is the government's agency that oversees lawful
11 immigration to the United States. We were formed in 2003 as
12 a part of the federal government's response to the 9-11
13 attack, which was consistent with the Homeland Security Act.
14 Our mission is to secure America's promise as a nation of
15 immigrants while providing accurate and useful information
16 to our customers, granting immigration and citizenship
17 benefits, promoting an awareness and understanding of
18 citizenship, and ensuring the integrity of the immigration
19 system.

20 USCIS protects the security of the American people
21 in the homeland by vigilantly enforcing the nation's
22 immigration and customs laws. As you probably know, March

1 1, 2003, USCIS officially assumed responsibility for the
2 immigration service function of the federal government. Of
3 course, this was done pursuant to the Department of Homeland
4 Security Act of 2002.

5 We were formed to enhance the security and improve
6 the efficiency of national immigration service by
7 exclusively focusing on the administration of benefit
8 applications. The first part of USCIS deals with the
9 adjudication process of all applications and petitions. In
10 the field, USCIS has 4 service centers, we have 4 regional
11 offices, and we have 250 facilities around the country.

12 The adjudication process is the main leg of USCIS.
13 They adjudicate all form types, all applications, and all
14 petitions. Also, USCIS -- another leg of USCIS is the FDNS,
15 which -- USCIS protects national security through the works
16 of an adjudication process and adjudication review of a
17 multitude of form types and applications for immigration
18 benefits. This process includes collection of biometrics,
19 biographics, and background investigations.

20 FDNS was created in 2004 by the U.S. Citizenship
21 and Immigration Services to support the effort to ensure
22 national security and the mission of providing the right

1 benefit to the right person at the right time and no benefit
2 to the wrong person. The division's top priorities are to
3 remove systematic and other vulnerabilities that impact the
4 legal U.S. immigration system, be a conduit between USCIS
5 and the law enforcement agencies and the intelligence
6 community. They also provide information-gathering
7 capabilities to help identify threats to national security
8 and public safety.

9 FDNS's primary mission is to detect, deter, and
10 combat immigration benefits fraud, to strengthen USCIS
11 efforts aimed at ensuring benefits are not granted to
12 persons who pose a national security threat to the United
13 States.

14 Another aspect of USCIS is the Field Operations
15 Directorate, which was established to oversee and manage the
16 day to day operations of the National Benefits Center, the
17 regional offices, 26 district offices, and 84 field offices,
18 which are located throughout the continental United States,
19 Alaska, Hawaii, Puerto Rico, Guam, Saipan, and the U.S.
20 Virgin Islands. We also have Field Office Operations
21 Directorates and we our staff include 4,471 federal
22 employees and 1,713 contractors that fulfil the occupancy of

1 those facilities. We also have four service centers, where
2 approximately 63 percent of all adjudication processes take
3 place.

4 Another leg of USCIS is the refugee-asylee
5 program, which is responsible for overseeing the planning
6 and the implementation of policies and activities related to
7 asylum and refugee issues, as well as immigration services
8 overseas. RAIIO offices play a critical role in expanding
9 citizenship and immigration benefits for eligible
10 individuals, exercising vigilance in matters involving fraud
11 detection and national security, sustaining effective
12 intergovernmental liaison and advancing USCIS strategic
13 priorities in the international arena.

14 RAIIO has 851 employees and is comprised of three
15 operational divisions, which reflects the directorate's
16 name. They are the Refugee Affairs Division, which is at
17 headquarters operations. This operation travels to conduct
18 refugee processing. They have the Asylum Division that has
19 eight domestic asylum offices. They have the International
20 Operations Division that has three overseas district
21 offices, which are located in Mexico, Mexico City, Bangkok,
22 and Rome. There are 29 field offices that make up RAIIO and

1 they are scattered abroad.

2 The records that USCIS maintains are kept in
3 primarily two systems and they're C3 and C4. Most of our
4 records -- the C3 system maintains all immigration records
5 on every applicant, petitioner, except for asylee, refugee,
6 and the verification. All other records are in C4. C4 is
7 for the naturalization, naturalization process. So all of
8 our records -- the majority of our records are maintained in
9 two systems, C3 and C4. We also maintain personnel records
10 as well on our employees.

11 Another arm of the USCIS is the Office of
12 Citizenship. The Office of Citizenship educates all of the
13 immigrants who are seeking naturalization. Over the last 3
14 years, the Office of Citizenship naturalized over -- in 2008
15 it was 1,045,539 applicants. In 2009 it was 743,715. In
16 2010 it was 675,967.

17 Each year USCIS welcomes approximately 680,000
18 citizens during the naturalization ceremonies across the
19 United States. These activities enhance the meaning of
20 citizenship and encourage immigrants and new citizens to
21 take an active role in their civic responsibilities.
22 Naturalization ceremonies have been held at locations

1 including the White House in Washington, D.C., Ellis Island,
2 the National Museum in New York, Fenway Park in Boston, the
3 USS Midway Memorial Museum in San Diego, and the Jefferson
4 National Expansion Memorial in St. Louis.

5 Another arm of USCIS is the Verification Division,
6 who verify the validity of immigration status of foreign
7 individuals working within the U.S. to would-be employers.

8 I'm going to share with you briefly some of the
9 statistics of USCIS over the last year. On a daily basis,
10 USCIS fulfils its promise to provide accurate and useful
11 information to our customers, adjudicate immigration and
12 citizenship benefits to detect and deter benefit fraud. We
13 promote awareness and understanding of United States
14 citizenship.

15 Every year USCIS receives approximately 6 million
16 immigration applications and petitions for legal review and
17 adjudication for a range of benefits. These benefits
18 include family-based petitions, employment-based petitions,
19 asylum-refugee processings, naturalization and citizenship,
20 special status programs, and document issuance and renewal.

21 On any given day, USCIS processes 30,000
22 applications for immigration benefits. They issue 6,000

1 permanent resident cards, which is also known as "the green
2 card." They adjudicate 200 refugee applications. They
3 adjudicate 230 asylum applications, naturalize 3,000 new
4 civilians and 27 new citizens who are members of the United
5 States armed forces.

6 USCIS serves a vital role in protecting the
7 security of our nation. To meet this responsibility, USCIS
8 conducts 135,000 national security background checks,
9 including collection of 11,000 sets of fingerprints at 129
10 application support centers.

11 Additionally, USCIS responds to 41,000 phone
12 inquiries and assists 12,000 customers who visit one of our
13 87 local offices and provides information to more than
14 200,000 customers who visit our web site.

15 Now we'll get to the Office of Privacy. The
16 Office of Privacy was created November 2007 as a result of
17 Secretary Chertoff's direction to the component leaders to
18 create a privacy office in some of the components. We
19 currently have three staff members. I make four. We have
20 been awarded two additional positions. At USCIS we are a
21 fee-based agency, so our funding is fee-based. It's not
22 appropriations.

1 I'm not sure if you're aware, but we recently
2 completed an IG review of the stewardship, the privacy
3 stewardship of USCIS. That review is still pending. If you
4 get an opportunity, look it up. It was pretty good. There
5 were some issues, but we're working through them.

6 When I first joined USCIS in 2007, when I came
7 into the office as the privacy officer I was told that we
8 had 25 to 30 PIAs that were delinquent. When I first saw
9 the PIAs and saw the fact that we hadn't had any PTAs that
10 was done and half our SORNs were not updated, I said this is
11 going to be a heavy load.

12 But after I got there, I realized that my goal and
13 what I had to do was to get in and dig in and see who the
14 players were. What I did was I got to know the program
15 managers -- first of all, I touched basis with the DHS
16 compliance office. We became very close. We work very
17 closely together. I got close with the program managers,
18 the system managers. We just sat down and talked about how
19 do we get these PIAs, SORNs, and PTAs done.

20 I was eager. I wanted to get it done. I didn't
21 really have a 3-year or 5-year or 7-year plan. I just
22 wanted to get it done. So the priority was already set for

1 me before I got there, because again they had a lot of
2 delinquency systems and the system was in operations and we
3 had to make sure that they were properly documented.

4 Working with DHS Compliance, we got right into it.
5 I mean, we got the first 2 or 3 done within I think the
6 first 6 months, and we continued to work on those PIAs until
7 we got most of them done. I think within the first year we
8 got about 9 to 12 of the PIAs done.

9 If you know CIS, it's a very, very busy component,
10 and by the time you get it done, get one of the PIAs done,
11 the operation has changed. We're doing new things. We're
12 trying to better the processes. So some of those PIAs would
13 fall back depending, based upon the changes of what the
14 operation is doing.

15 One of the additional things that happened coming
16 to the CIS and taking on all of the PIAs, PTAs, and SORNs
17 was that we had -- there was no policy or there wasn't a
18 policy that everybody was adhering to. So we had incidents
19 that popped up in Texas and Vermont. So in the midst of
20 doing PIAs, I had to get on the plane and fly out to Texas
21 and fly out to Vermont. The compliance team, the DHS
22 compliance team, actually went out with me to the National

1 Records Center. We did privacy audits.

2 I say that to say that, with all of the PTAs that
3 we had to do and the breaches that were occurring, it was
4 obvious that CIS had a lot of work that had to be done
5 outside of compliance. They had a serious privacy issue,
6 and being there was certainly going to be a task.

7 Again, I flew out, did training. We trained and
8 we trained and we trained. Everywhere we went, we trained.
9 Most of the staff members had not heard of privacy. They'd
10 heard of it, but they didn't know what privacy was. So we
11 started behind the eightball, teaching them what privacy
12 was, teaching them their responsibility in terms of privacy,
13 utilizing the Fair Information Practices Principles.

14 It was a lot of work trying to do the PIAs, the
15 PTAs, the SORNs, and now the breach part. As I worked with
16 the Department to get the PTAs done, I came back. Based
17 upon my discussion with the staff out in the field, I
18 developed a policy for how you handle PII within USCIS,
19 because there are some specific intricacies within CIS that
20 I guess it was difficult for them to understand in terms of
21 the DHS policies. So we crafted the policy to be
22 specifically to USCIS, but at the same time making sure that

1 the DHS policy was adhered to as well.

2 Immediately after I got this done, there was some
3 pushback, but the policy went through and you could see the
4 change in USCIS right from the start. I mean, people
5 started adhering to the policy. They started -- a lot of
6 questions came in: Well, how do I do this, how do I do
7 that? This PII, that PII.

8 Of course, a lot of emails came in. So we
9 established a mailbox so staff could send in all of their
10 complaints, inquiries, etcetera, regarding privacy. Over a
11 period of time, we had our incidents spiked, and at the same
12 time our PTAs were getting done. Shortly after that, I
13 hired, I think in 7 months, I had an opportunity to hire my
14 deputy. Things slowed down just enough so that I could hire
15 the deputy.

16 Once she got in, again it was -- I felt that we
17 had the PTAs going well. I thought the best chance of
18 making CIS a success was to really, really hit the training
19 part really hard, so that we would have less issues in terms
20 of privacy down the road. I amended the policy probably
21 twice to allow -- the initial policy was very strict. It
22 kind of slowed things down. So I kind of lifted a little

1 bit of it so that staff could send emails through the DHS
2 firewall with the exception of the Social Security number.
3 Any email that was sent with the Social Security number
4 required encryption and if it didn't have the Social
5 Security number then you could send it within the firewall.
6 But prior to that, everything had to be encrypted and that
7 kind of slowed everything down within USCIS.

8 As we continued to build the program, I was
9 awarded another staff member and we were up to three staff
10 members. Again, I was -- the PII process was moving well --
11 I mean, the training part was doing well at the time, and I
12 took one more leg, one more strike at the training part and
13 we went out again. That year, I think we did 28 different
14 sites where we did instructor-led training. We went out and
15 that year we trained 17,500 employees of 18,000. We really
16 did well.

17 When we go out, one of the things that we did was
18 we engaged the leadership, the employees, and basically told
19 them that the privacy program was their program. We wanted
20 to integrate their need into the program. When we were
21 providing them privacy training, we didn't want to provide
22 them a generic privacy training. We wanted to make sure

1 that the privacy training was touching what they did on a
2 day to day basis. So we developed training that impacted
3 upon what they did every day.

4 We integrated what they were doing. We used
5 analysis. We used the breaches that was occurring to teach
6 them what not to do and what to do, utilizing analysis of
7 those situations and asking questions: What would you do in
8 these situations? So that not one or two people would
9 learn, but everybody in there, in the session, was learning.
10 Everybody was engaged. We got a lot of questions.

11 I will share one thing with you about the IG
12 report and that would be this. Over almost 4500 people out
13 of the 7900 employees submitted comments or submitted
14 statements about the privacy program. A lot of it, they
15 liked what was going on, they wanted more privacy training,
16 they wanted different iterations of it. They wanted more
17 privacy. We thought that was really, really a good thing.

18 As we continued to provide the training, we got
19 more and more -- the breaches, the breach number of course
20 went up. As the education goes up, the number goes up. So
21 our breaches went up. But as we started to get out and do
22 the breach notification, get out and talk to the staff about

1 establishing not just a notification, but whenever there's a
2 credit monitoring -- we established a whole entire process
3 where if an individual is affected or impacted, where their
4 financial situation is going to be impacted, we have a
5 situation set up now where the individual, if we determine
6 that it warrants breach notification and credit monitoring,
7 that process is so fluid that we just contact the program,
8 let them know that the individual needs to be notified, that
9 they need credit monitoring, and it just flows. We have
10 absolutely no problems. From A to Z, it happens very
11 fluidly.

12 I also established -- because of that, I
13 established a breach policy that also is a step by step
14 process as to what you do, utilizing the DHS PIHG, Privacy
15 Incident Handling Guidelines, and took that and then broke
16 it down specifically for USCIS, identifying who contacts who
17 within the programs, ensuring that the ball is not dropped
18 and that the process is fluid.

19 I would be remiss if I didn't mention one of our
20 larger initiatives that's going on and that's the
21 transformation. USCIS, if you know, USCIS has millions and
22 millions of A-files. The process that USCIS is going

1 through is migrating from a paper based process to an
2 electronic process. It's similar to what you would do at
3 your bank. An individual will be able to go to a kiosk and
4 they'll be able to initiate the process of their benefit
5 application process. They put all the information in
6 electronically. They can scan the information
7 electronically, and it goes to USCIS.

8 The thing is now is that once it goes fully
9 electronic USCIS will not be keeping the paper. The paper
10 will be sent back to the individual. But again, the
11 individual can update their application, they can see what
12 their status is, etcetera. They don't have to send in
13 letters or call in to say what is the status of my
14 application.

15 As the privacy officer for USCIS, I'm always
16 looking to see how we better our program. With that, I have
17 -- where I'm seated at USCIS as a part of the executive
18 staff, I have an opportunity to reach out and touch all of
19 the top leads throughout the program. So I think from that
20 standpoint privacy gets the visibility again. But with the
21 visibility, you have to keep, you have to keep saying it.
22 You have to keep saying it, because I found out that a lot

1 of times you can speak, you can talk about privacy, and you
2 mention it and sometimes some people still don't get it.

3 So each and every day or each and every week I am
4 always talking about privacy, something that's going on or
5 something that we're doing within the program to make sure
6 that privacy is getting the necessary visibility so that the
7 program flourishes.

8 I can say today that USCIS privacy program is
9 alive and well. I think it's doing well. It is recognized
10 throughout the country, and the leadership throughout USCIS
11 recognize the privacy program. All I can say is that the
12 program is flourishing.

13 With that, I conclude my statement.

14 CHAIRMAN PURCELL: Thank you very much, Mr.
15 Hawkins.

16 I had one question. It's kind of a combination
17 deal. One of the things about immigration, refugee status,
18 asylum, and a lot of the people you're dealing with is the
19 collection of quite sensitive information, whether it's
20 health, religious, political, or otherwise. Can you explain
21 to me the way that you handle both highly sensitive
22 information and also biometric information, which I would

1 include in that category as well?

2 Is it cached in a separate database outside of the
3 C3 and C4? I love "C4". That's an explosive. I'd put it
4 in there probably. "C3" because it's nonprofit, right?

5 (Laughter.)

6 I'm just curious about how you handle that,
7 because it occurs to me you must have a tremendous amount of
8 very sensitive information. One, is there a data
9 classification for that? Two, are there separate
10 procedures, security procedures and handling procedures,
11 access controls, etcetera, in order to review it? Three, is
12 it locked up in a way that prevents its disclosure or
13 inadvertent sharing with people who are unauthorized to see
14 it? Those kinds of questions come to mind.

15 MR. HAWKINS: In terms of the sensitive
16 information, I mentioned C3 and C4. We do have additional
17 systems that house the biometrics. We do have biometric
18 systems that house fingerprints. So those systems do
19 require passwords, user's name and password, so it's
20 protected.

21 I will also admit that, in terms of C3 and C4,
22 it's a legacy system and there are some issues with C3 and

1 C4. But we are working on migrating those systems through
2 some security channels, whereas in the past C3 and C4 didn't
3 have the proper security that it needed. But now through
4 the person-centric query and the enterprise service bus that
5 USCIS has recently implemented, that requires user's name
6 and password to access C3 and C4 data.

7 CHAIRMAN PURCELL: It sounds like a bit of a work
8 in progress, though, for some of the more sensitive stuff,
9 too.

10 MR. HAWKINS: It is a work in process, but the
11 enterprise service bus is actually encompassing all of
12 USCIS's system, meaning that every access to all of the
13 legacy databases requires you to go through the enterprise
14 service bus to access those systems. So you would have to
15 have a user name and password to access any of the legacy
16 systems.

17 CHAIRMAN PURCELL: Right, right. Okay.

18 Ramon.

19 MR. BARQUIN: Don, knowing that you started from
20 zero, I commend you for how far you've gotten. But that's a
21 very good segue to my question, which is I'd like to just
22 get a sense -- I don't know specifics -- but the number of

1 databases in the adjudication process for citizenship,
2 naturalization, green card, etcetera? The databases that
3 you are automatically needing to query, touch base with,
4 inquire, whatever, exchange information with, of those
5 percent-wise how many are within USCIS and how many are
6 within DHS?

7 Then you've got, I know, dealing with other law
8 enforcement agencies, both federal and state and local. How
9 does that work in general?

10 MR. HAWKINS: The majority of systems that we
11 utilize to make a benefit decision is within USCIS. I don't
12 know of any particular system that we require access to to
13 make a benefit decision. There are systems where we work
14 with some of the other components, such as CBP, to determine
15 if an individual has committed any crime, maybe through TEKS
16 or IBIS or something like that.

17 But in terms of the benefit decision itself, most
18 of the systems that we utilize are CIS systems.

19 MR. BARQUIN: Okay. I guess I was going -- to
20 just follow up, being a naturalized citizen myself, I know
21 that my file was this big (indicating) when I finally -- and
22 I'm assuming --

1 MS. CALLAHAN: Did you FOIA? Did you get it in a
2 timely fashion?

3 MR. BARQUIN: This was long ago.

4 But the need -- and by the way, I know that in
5 theory it is done, and if it isn't done then it shouldn't be
6 done, which is check with databases or files of law
7 enforcement agencies to make sure that the individual has
8 not committed crimes or whatever. So I'm just curious how
9 that is being done now, if it is being done electronically?

10 MR. HAWKINS: In terms of the naturalization
11 process or the process of a legal permanent resident or any
12 benefit, what we're beginning to do and we have not -- we
13 haven't actually initiated this yet -- is the recurrent
14 vetting, which requires just the check to ensure that the
15 individual has not committed a crime since they initiated
16 their initial paperwork or application.

17 Prior to that, what's happening is that the
18 application is being vetted up front, meaning that when the
19 background check is done it's checked to determine if
20 there's a crime been checked -- or a crime has been
21 committed, early on.

22 CHAIRMAN PURCELL: Mr. Hawkins, in that process do

1 you use biometrics primarily? Do you use a fingerprint
2 matching algorithm to do that?

3 MR. HAWKINS: The background check is both, the
4 biometric and the fingerprint.

5 MS. CALLAHAN: Biographic.

6 MR. HAWKINS: Biographic, yes.

7 CHAIRMAN PURCELL: And biometric.

8 Howard.

9 MR. BEALES: You mentioned that there's the two
10 databases for immigration and naturalization records, the C3
11 and the C4, and I gather a lot of the records exist in both
12 systems?

13 MR. HAWKINS: No. The naturalization process is
14 C4. It's strictly for naturalization. All of the other
15 benefits are in C3.

16 MR. BEALES: Okay. But presumably all those
17 people started out as immigrants before being naturalized.
18 So they're in C3 and then --

19 MR. HAWKINS: I would assume that to be true.

20 MR. BEALES: And then they're also in C4?

21 MR. HAWKINS: Yes. If they go from -- say if
22 they're seeking another benefit and then they have a chance

1 of status whereas they are seeking naturalization, then they
2 would be in C3 and then they would be in C4 as well. Their
3 information would be in both.

4 MR. BEALES: Okay. And I guess what I was
5 interested in is how is that process managed and how is the
6 updating of that information managed where it's in two
7 places at once?

8 MR. HAWKINS: They utilize the information that's
9 in C3 and they compare the information to make sure it's
10 consistent. When they submit the application for the
11 naturalization, they utilize the same information. I guess
12 if the information that the individual is submitting for the
13 naturalization process is consistent with what they utilized
14 in the initial benefit, then they would do a comparison with
15 that information.

16 MR. BEALES: And at the beginning that's easy.
17 When I first move into the C4 database because I've applied
18 for naturalization, everything's consistent. What happens
19 when I'm still waiting to be naturalized and I report a
20 change of address or whatever else changes in the record?

21 MR. HAWKINS: Once you start the naturalization
22 process, you're in C4. So all of your change would occur in

1 C4. But the --

2 MR. BEALES: So C3 is just obsolete at that point?

3 MR. HAWKINS: Once you get into the naturalization

4 process, yes.

5 MR. BEALES: Okay, but it still exists in that

6 database?

7 MR. HAWKINS: Yes.

8 MR. BEALES: Okay.

9 Okay. That was what I was wondering. Thank you.

10 CHAIRMAN PURCELL: Retention issues come up, but

11 I'm going to skip over that for the moment.

12 Larry.

13 MR. PONEMON: The communal microphone, thank you.

14 Firstly, thank you for your service, by the way.

15 I counted 23 years in the Air Force?

16 MR. HAWKINS: Yes.

17 MR. PONEMON: Good job. We appreciate it.

18 Just a general question. You talked a little bit

19 about compliance. Not a little bit. It seems like a lot of

20 the focus in your organization is compliance, training,

21 getting people up to speed. But what are some of your worst

22 privacy nightmares? Let me give you an example. We had a

1 little bit of a conversation; I think Jim brought up to DNA
2 testing, the screening controversy. Are you involved in
3 those kinds of decisions? Are you looking at a technology
4 like that before it actually becomes a serious
5 consideration? Does that constitute one of your privacy
6 nightmares?

7 MR. HAWKINS: If the technology is --

8 MR. PONEMON: You know, great technology, privacy
9 issues abound.

10 MR. HAWKINS: Generally, if something like that is
11 on the horizon it is brought to my attention. The
12 particular situation that you're speaking of, it was brought
13 to my attention.

14 MR. PONEMON: So there was vetting, an appropriate
15 level of vetting in your opinion, to basically get from
16 concept to potentially testing? I don't know enough of the
17 facts. I don't want to rely on the major media, but I
18 assume that --

19 MS. CALLAHAN: Always a good source, Larry.

20 MR. PONEMON: It's always a great choice.

21 (Laughter.)

22 But it would seem to me that there was a decision

1 made and then there was a lot of controversy around that.
2 But you considered it, so that's a good fact. In other
3 words, someone in your organization or you in particular
4 considered the privacy impact and decided that it would be
5 okay to kind of move to the next phase?

6 MR. HAWKINS: Yes. The program brought it to my
7 attention and, based upon their description and analysis of
8 how they proposed that it may be used, I didn't have an
9 issue with it.

10 MR. PONEMON: Thank you.

11 CHAIRMAN PURCELL: Joanne.

12 Ms. McNABB: Thank you for the good work you're
13 doing. I recognize the sort of trajectory from where you
14 started. I think that's pretty common among new privacy
15 officers in organizations that haven't had them before. It
16 sounds like you're doing a good job.

17 I just wanted to confirm what I assume when you
18 said that as the training went, developed, the number of
19 incidents developed. I would assume that's because
20 awareness developed. It's not like their practices are
21 getting worse. It's just now they recognize that there was
22 an incident.

1 MR. HAWKINS: Yes. Their awareness was very high.
2 When we go out and train, at the end of a training session
3 everybody's excited and they're coming up, they're sharing
4 what they're doing and not doing. Do we need to do this, do
5 we need to do that? I want to make sure I'm doing the right
6 thing.

7 So when they see something inconsistent with what
8 we've been telling them to do, then they're reporting it.

9 Ms. McNABB: I've seen in organizations you've now
10 trained up a little army of privacy police who are alert.
11 And that's good, but it also does mean that the incidents go
12 up, and that's something that a privacy officer has to
13 manage with the higher-ups to set their expectations.

14 MR. HAWKINS: Absolutely. Just for a point of
15 clarification, I just wanted to make sure that everybody
16 understands that C3 and C4 is Claims-3 and 4.

17 CHAIRMAN PURCELL: That's good. I'm glad, given
18 the alternative.

19 (Laughter.)

20 Thank you, Donald, very much for your time. I
21 appreciate it. Thank you for joining us today, and if we
22 have any questions we'll address them back to your office.

1 Thanks very much for helping us today.

2 MR. HAWKINS: Thank you.

3 CHAIRMAN PURCELL: I'd like to call our next
4 speaker, who is Eric Leckey. Eric is the Associate Director
5 for Privacy Compliance and Program Development in the DHS
6 Privacy Office. Eric's focus is on the development and
7 implementation of the full sweep of Department privacy
8 compliance documentation under the Privacy Act, the Computer
9 Matching and Privacy Protection Act, the Government Act, and
10 the Homeland Security Act.

11 Prior to joining the Privacy Office staff, Mr.
12 Leckey was a Senior Associate and Engagement Manager in the
13 privacy practice at PriceWaterhouseCoopers, where he
14 provided privacy support for the DHS Privacy Office. He has
15 also served in various positions both in the Department as
16 well as in the White House.

17 Mr. Leckey is reporting today on privacy
18 protections in place for the Department's use of social
19 media. Eric, welcome. Please proceed.

20 PRIVACY PROTECTIONS FOR DHS USE OF SOCIAL MEDIA,

21 BY ERIC LECKEY

22 MR. LECKEY: Thank you. Chairman Purcell and

1 members of the Committee: Thanks for the opportunity to
2 brief you today on the Privacy Office's efforts to build
3 privacy protections into the Department's social media tools
4 and initiatives.

5 Before I start my social media brief, I wanted to
6 respond to a question that Mr. Barquin had at the September
7 2010 DPIAC meeting on computer matching agreements and the
8 Data Integrity Board. As Mary Ellen indicated then, the
9 Privacy Office has been reconstituting the Data Integrity
10 Board to make it more effective in executing its statutory
11 obligations under the Privacy Act. Those duties, among
12 others, include reviewing and approving all written computer
13 matching agreements for receipt or disclosure of the
14 Department's Privacy Act records -- excuse me -- Privacy Act
15 records for matching programs; reviewing all matching
16 programs in which the Department has participated during the
17 year as either a source or recipient agency, to determine
18 and to assess the costs and benefits of each program; and
19 reviewing all matching programs in the Department, including
20 the policies and procedures for safeguarding security and
21 proper disposal of records under those matching programs.

22 Computer matching activity is any computerized

1 comparison of two or more automated systems, of which one
2 must be federal, for the purpose of establishing the
3 eligibility for cash or in-kind assistance or payments or
4 recovering debts under federal benefit programs.

5 Proposed membership of the new reconstituted Data
6 Integrity Board includes: the Chief Privacy Officer as
7 chairperson; the Inspector General by statute; and the
8 Officer for Civil Rights and Civil Liberties to further
9 coordinate between our two offices as called for under the
10 Homeland Security Act; the Chief Information Officer of the
11 Department; and the deputy component heads of the Department
12 who currently have computer matching agreements. Those
13 include U.S. Citizenship and Immigration Services, the U.S.
14 Coast Guard, Federal Emergency Management Agency, and
15 Immigration and Customs Enforcement.

16 The Privacy Office has formalized these
17 individuals and processes in a delegation of authority,
18 management directive and instruction. All three are
19 currently drafted and in review at the Department level.

20 That does conclude my response to the record that
21 I read in preparation for this meeting and heard at that
22 meeting in 2010.

1 Mr. Chairman, I'm happy to answer any questions
2 now on that or we can save all until the end.

3 CHAIRMAN PURCELL: Ramon, are you satisfied?

4 MR. BARQUIN: I do have a question, but I can
5 either do it now or at the end. You tell me?

6 CHAIRMAN PURCELL: Let's take care of it now while
7 we're on this subject.

8 MR. BARQUIN: First of all, thank you.

9 MR. LECKEY: Sure.

10 MR. BARQUIN: We've been on this for a while. But
11 the question is -- and I recall having asked the question --
12 is this board exclusively and specifically tied to matching?
13 Because if it is, then it is an opportunity to try to go
14 beyond that at the Department level. I just wanted to know.

15 MR. LECKEY: I appreciate that. I will say that
16 the Data Integrity Board does have a statutory mandate, and
17 so what I read today is part of that. There is a piece of
18 that, in looking at the record, that does allow for the
19 reviewing of Department policies and procedures for
20 safeguarding security and the proper disposal of records.

21 Whether there's some wiggle room there to address
22 the direct concern, I would sort of defer to the chairperson

1 when that happens or General Counsel's office and so on.
2 That would generally be the area that I see as most
3 applicable to what you were referring to. But I would sort
4 of leave it to them at that time.

5 MS. CALLAHAN: Ramon, I think the reconstituted
6 DIB will provide us some insights into broader policy
7 issues, and I think that that will hopefully be a useful
8 tool, and we're implementing it on a de facto basis at this
9 point.

10 MR. BARQUIN: Thank you.

11 CHAIRMAN PURCELL: Eric, proceed.

12 MR. LECKEY: Thank you.

13 With respect to privacy protections built into
14 social media, the Privacy Office has been actively engaged
15 in ensuring that privacy protections are built into new and
16 existing social media tools and initiatives at the
17 Department and that we're at the table for all social media-
18 related discussions.

19 The Privacy Office held its first public workshop
20 on social media in June 2009. I know you'll remember.
21 Since then, the Privacy Office has been a leader in
22 compliance and policy discussions related to the development

1 and launch of social media tools and initiatives. From the
2 beginning, the Privacy Office has concluded that the public
3 user fully expects privacy protections while interacting
4 with the Department.

5 To ensure that the Department's use of social
6 media tools and initiatives complies with federal laws,
7 executive orders, regulations, and policies, and to apply
8 standards consistently across the Department, the Privacy
9 Office has led an effort to establish a Department-wide
10 Social Media Compliance Steering Committee, which is now up
11 and running.

12 The committee consists of the Office of General
13 Counsel, the Office for Civil Rights and Civil Liberties,
14 the Privacy Office, Office of Public Affairs, the Chief
15 Information Security Office, and Office of Records
16 Management. The committee collaborates to ensure that all
17 documents related to social media tools and initiatives are
18 cleared and to ensure that compliance issues are considered
19 and coordinated before implementation.

20 Because of the depth and diversity of social media
21 tools and initiatives, we knew that we would need to develop
22 an approach that would allow us to manage volume. To

1 facilitate this, we developed the social media PTA for use
2 in external affairs and public outreach. The social media
3 PTA asked the end user a basic set of questions about the
4 social media tool or initiative to begin to narrow down
5 whether it will be covered by a Social Networking
6 Interactions and Applications PIA or a Unidirectional Social
7 Media Applications PIA and to document that discussion.

8 If the former, the end user responds to the
9 questions on the PTA that focuses on bidirectional, two-way
10 information flow to and from the Department. If the latter,
11 the end user responds to questions on the PTA that focuses
12 on unidirectional, one-way dissemination only from the
13 Department to the end user outside the Department.

14 The privacy protections for each social media tool
15 and initiative are exclusive to one of the two categories I
16 just mentioned, bidirectional or unidirectional, within the
17 sphere of external affairs and public outreach.

18 The Social Networking Interactions and
19 Applications PIA is intended to cover videos and images,
20 such as YouTube and Flickr, blogs such as Twitter and
21 Googleblogger, and social networking such as Facebook and
22 LinkedIn.

1 Key privacy protections built into this use of
2 social media includes: not actively soliciting PII;
3 collecting only the minimum amount of information which the
4 Department receives to accomplish a purpose required by
5 statute, executive order, or regulation, if in fact there is
6 a previously published Privacy Act System of Records Notice;
7 no searching for or by PII; no active friending or related
8 activity unless it is with another government entity at the
9 federal, state, or local level -- tribal's obviously in
10 there; international partners as well.

11 We do have a waiver process in place if entities
12 believe that their mission will require them to extend that,
13 and we have considered a couple. But the Department may in
14 fact accept friend requests from outside users. So the idea
15 there is the Department will not proactively reach out and
16 friend, but if the Department is sent a request we may
17 accept it.

18 Access restrictions to access the social
19 networking tools and initiatives; posting of privacy policy
20 and-or privacy notice on the third party web site itself if
21 that's feasible; reviewing the third party privacy policy to
22 determine if it is acceptable for the Department's use; pop-

1 ups when diverting away from the DHS page; DHS branding and
2 logo to ensure that the public user understands that they're
3 interacting with the Department; and a National Archives and
4 Records Administration-approved records retention schedule.

5 If information-sharing is done for official
6 purposes and under a routine use, it may be shared outside
7 the Department. User training; Office of Public Affairs
8 approval for those information releases in all cases; and an
9 auditing component through the privacy compliance reviews
10 and the Social Media Compliance Steering Committee. You
11 heard from Jamie Pressman at the September 2010 meeting on
12 our privacy compliance reviews.

13 With respect to the unidirectional social media
14 application PIA, it is intended to cover Widgets and RSS
15 feeds, SMS texts, audio files, podcasts, and those on the
16 dhs.gov domain for the purpose of one-way dissemination of
17 information outside the Department.

18 The risks were lower with this use because the
19 Department was strictly pushing out information, not
20 receiving, and focuses heavily on public profile and public-
21 related information associated with users if one in fact
22 does exist for that specific social media tool.

1 Key privacy protections built into this use of
2 social media were similar, but somewhat different, and did
3 include: access restrictions again; posting of a privacy
4 policy and-or privacy notice on the web site or the
5 application itself if feasible; reviewing the privacy policy
6 to determine if it was acceptable for Department's use;
7 again, DHS branding and logos if possible; records retention
8 schedules approved by NARA; user training; Office of Public
9 Affairs Approval for information releases in all cases;
10 redress, in both cases through the Office of Public Affairs;
11 and again the auditing component through privacy compliance
12 reviews and the Social Media Compliance Steering Committee.

13 One specific use outside of public dialogue,
14 external affairs, public outreach, that I want to bring to
15 your attention is the Department's use of other operational
16 uses of social media. One that I want to call out
17 specifically is the Office of Operations, Coordination, and
18 Planning's publicly available Social Media Monitoring and
19 Situational Awareness PIA. In this case, the National
20 Operations Center, which is part of the Office of
21 Operations, Coordination, and Planning, reviews publicly
22 available social media to provide situational awareness and

1 establish a common operating picture pursuant to their
2 statute. So they have a statutory authority to develop a
3 common operating picture for the federal government's
4 leaders to use and to provide situational awareness on an
5 updated basis.

6 To build privacy protections into this initiative,
7 the Office of Operations, Coordination, and Planning was not
8 permitted to post any information, actively seek to connect
9 with other internal or external users, accept other internal
10 or external users personal invitations to connect, or
11 interact on social media sites.

12 Under this initiative, the Office of Operations,
13 Coordination, and Planning was permitted to establish user
14 names and passwords so that they may form profiles and
15 follow relevant government, media, and subject matter
16 experts on specific social media sites, in order to use
17 search tools under established criteria and search terms for
18 monitoring the supports providing situational awareness and
19 a common operating picture, again pursuant to their statute.

20 Furthermore, PII on specific categories of
21 individuals were permitted to be collected when it lends
22 credibility to the report that facilitates coordination

1 between federal, state, local, tribal, territorial, foreign,
2 or international government partners: the U.S. and foreign
3 individuals in extremis situations involving potential life
4 and death circumstances; senior U.S. and foreign government
5 officials who make public statements or provide public
6 updates; U.S. or foreign government spokespersons who make
7 public statements or provide public updates; U.S. and
8 foreign private sector officials and spokespersons who make
9 public updates; names of anchors, newscasters, or on-scene
10 reporters who are known or identified reporters in their
11 post or article or who use traditional and-or social media
12 in real time to keep their audience situationally aware and
13 informed; current and former public officials who are
14 victims of incidents or activities related to homeland
15 security; and last but not least, terrorists, drug cartel
16 leaders, and other persons known to have been involved in
17 major crimes of homeland security interest, mass shooters,
18 the Virginia Tech or Fort Hood incidents, to name a couple,
19 who are killed or found dead.

20 Due to this new collection of PII and the ability
21 to retrieve this PII by personal identifier, a system of
22 records was published. It's DHS OPS 004, publicly available

1 Social Media Monitoring and Situational Awareness System of
2 Records. This specific initiative was born out of many
3 events and incidents and disasters over the past year. As
4 you know, we experienced the Haiti disaster and were
5 involved with that, the Olympics and the BP oil spill.
6 While we have separate PIAs on these specific social media
7 initiatives, as it relates to this specific initiative with
8 respect to social media monitoring the PIA will allow the
9 Office of Operations, Coordination, and Planning to fulfill
10 its mission while protecting privacy in the process.

11 That specific initiative was a good combination of
12 the social media compliance process and our privacy
13 compliance review process, which again you were briefed on
14 in September 2007.

15 With that -- sorry, September 2010.

16 With that, Mr. Chairman and members of the
17 committee, thank you for the opportunity to brief you today
18 on social media tools and initiatives and privacy compliance
19 and privacy protections that we've built in. That concludes
20 my formal briefing and I'm happy to take questions.

21 CHAIRMAN PURCELL: Thank you, Mr. Leckey. We
22 appreciate your input.

1 Joanne.

2 Ms. McNABB: I got excited about something you
3 said and I think I then was not able to take in as you went
4 on about it. When you were talking about the Office of
5 Operations, Coordination, and Planning, were you saying that
6 what they are doing is surveiling social media sites,
7 looking for specific people and events?

8 MR. LECKEY: So there are public aspects to
9 certain social media sites.

10 Ms. McNABB: Yes.

11 MR. LECKEY: Within its mission and within its
12 statute, to review different sources of information to
13 provide that common operating picture and those situational
14 awareness reports, they do pay attention to traditional news
15 media as we see it -- CNN, Fox News, the traditional sort of
16 across-the-board news networks, print media, social media
17 networks, again where that information is made public, where
18 it applies to what it is that they're doing.

19 Ms. McNABB: So obviously if people's privacy
20 controls are pretty wide open, that's pretty easy for anyone
21 to do. But I think I sort of heard you say that they may
22 also be creating profiles that would allow them to friend

1 their targets and then get more information from their
2 social media sites?

3 MR. LECKEY: The idea is to not do that. That is
4 our documented -- yes, and I'll clarify that for you. Under
5 the Office of Operations, Coordination, and Planning, no,
6 that is not an acceptable practice that's in our Privacy
7 Impact Assessment. The confusion I think that has been
8 created during my brief is the social networking
9 interactions and applications PIA for purposes of basically
10 interacting, sort of that two-way, for public outreach,
11 external affairs, and that sort of thing -- in those cases,
12 that is a very, very different use of social media than in
13 the Office of Operations and Coordination, and there's a
14 hard line between the two. It's a big wall. There's not an
15 intersection there.

16 I wanted to sort of explain several of the
17 different angles that we've gone with privacy compliance and
18 building in privacy protections to the different social
19 media projects around the Department. But to clarify, no,
20 those two are not related in terms of their use.

21 One thing I do want to sort of also mention with
22 respect to the Office of Operations, Coordination, and

1 Planning initiative, which I'll just now call "the OPS
2 initiative," if that'll work for everyone, is that they're
3 not looking for people. That is an event-based activity.
4 So the idea is not to focus on the individual. The idea is
5 to focus on the event and the information that's provided
6 publicly related to that event.

7 Ms. McNABB: And will these two -- I've read, I
8 thought, pretty much all of your social media, the workshops
9 and the policies that I was able to find, because we've just
10 ventured into that for the California Office of Privacy
11 Protection and we're feeling anxious about something going
12 wrong.

13 But I don't think I've seen those PIAs. If I just
14 go to the PIA page they'll be there?

15 MR. LECKEY: I'm excited to present you with a
16 unidirectional one. It'll be on our web site today or
17 tomorrow. We've taken that action. It should be published.

18 Ms. McNABB: And the bi is already there?

19 MR. LECKEY: The bi has been there since
20 September, yes.

21 Ms. McNABB: Somehow I didn't --

22 MR. LECKEY: And OPS since June. I will tell you

1 there are a number of them on there. But the areas of focus
2 are under -- if you go to our web site, are under DHS-wide.

3 Martha, we can probably also provide them if we
4 want to do it by email.

5 Ms. McNABB: I can find them.

6 MR. LECKEY: Okay. DHS-wide and then Office of
7 Operations, Coordination, and Planning.

8 Ms. McNABB: And I've seen all the policies that
9 you link to from your Facebook page, for example.

10 Thank you.

11 MR. LECKEY: Sure.

12 CHAIRMAN PURCELL: You can't friend, but you can
13 like.

14 MR. LECKEY: Are there any other questions?
15 Howard?

16 MR. BEALES: You mentioned that what you're
17 looking for is events-based information, not person-based
18 information?

19 MR. LECKEY: Right.

20 MR. BEALES: Does this mean you'd look for all of
21 the people, all of the people who signed up on the Facebook
22 page or whatever to go to the Rally to Restore Sanity?

1 MR. LECKEY: I think what we don't want to focus
2 on is the word "look." So what we're doing is we're
3 remaining aware through those vehicles which provide
4 information through that tool. We're not going and
5 specifically seeking anything out. And this can be
6 everything from blog posts to whatever information would be
7 provided in a public forum, not focusing on the individual,
8 would we take that information or use it for that purpose.

9 MS. CALLAHAN: Howard, your example on the Rally
10 to Restore Sanity, the only thing that OPS would ever be
11 worried about there would be to the extent that there is
12 some sort of event that affects national security, there is
13 a riot or something like that. So they would watch the
14 Twitter feed, not to know what the Roots were saying or what
15 Jon Stewart was saying. They would go and do it to say,
16 there seems to be a problem at L'Enfant Plaza, there seems
17 to be -- people are tweeting that they've fallen down the
18 escalator stairs at L'Enfant Plaza.

19 I don't know if -- but that would be what they
20 would be looking for, is the reaction. There are tweets
21 we're having a problem at L'Enfant Plaza; perhaps you should
22 notify Metro.

1 MR. BEALES: Okay, and I guess --

2 MS. CALLAHAN: We don't care who's attending it.
3 We care to the extent that there is impact related to
4 national security or operational awareness.

5 MR. BEALES: Okay. And I can see that in sort of
6 the real-time, sort of the real-time paying attention. But
7 suppose there is an incident that could have been a
8 terrorist incident. Then suddenly all of that's going to
9 become very person-focused.

10 MS. CALLAHAN: That's not the authority of the
11 Office of Operations.

12 MR. LECKEY: So in that case that information
13 would not get collected on the person-focused activity. It
14 would be focused exclusively on the event and providing what
15 they call media monitoring capability reports on the event.
16 It would not be focused on the individual or providing or
17 basically ingesting information on the individual, providing
18 reports on the individual. It is an event --

19 MR. BEALES: Let me spin out what I'm trying to
20 ask this way, because I get that it's about the event, okay.
21 We're monitoring the event. I don't know what it is,
22 somebody's rally to do something. And we're paying

1 attention to whether the escalator broke, I get that, in
2 real time. And then something bad happens at this event.

3 Suddenly, the names of the people who identified
4 themselves, or the identifiers about on the Facebook page
5 for people who liked that event, whatever, have a whole new
6 relevance. Are you saying nobody uses that information,
7 nobody looks there? Or are you saying somebody else does it
8 under a different set of authorities and restrictions and
9 not OPS?

10 Once there's a real operation, it's not OPS any
11 more? I'm not understanding.

12 MR. LECKEY: Those are very good points. At some
13 point when those specific, more specific person-focused,
14 depending on the event, I think the FBI -- other
15 organizations and entities with appropriately aligned
16 authorities would then handle that information.

17 MS. CALLAHAN: Once it becomes a law enforcement
18 investigation or related event, then the Office of
19 Operations provides the situational awareness: This has
20 happened. We'll continue to monitor it and say, okay, the
21 escalator remains broken or whatever. If you say it's a
22 terrorist attack, then that goes to the Federal Bureau of

1 Investigation and other law enforcement entities.

2 The law enforcement entities, FBI among others, do
3 receive the media monitoring. The idea is to give just-in-
4 time or real-time identification of events. That's OPS'
5 authority. But OPS is not an investigatory branch. It's
6 not an enforcement element of the federal government. So
7 that's why it would shift to that.

8 MR. BEALES: So it's not hanging onto the list of
9 people who were there?

10 MS. CALLAHAN: Right.

11 MR. BEALES: Because presumably one of the early
12 things the FBI wants to do is, okay, who was there?

13 MS. CALLAHAN: So the FBI could get it under their
14 own authority. I'm using "FBI" generically.

15 MR. BEALES: I understand, right.

16 MS. CALLAHAN: They could get it under their own
17 authority, yes.

18 MS. RICHARDS: Which is why it's a very narrow
19 group of seven pieces of PII that they can actually collect,
20 and that we have now audited twice on them and they are up
21 for their next audit in June. And we've scrubbed them and
22 reviewed them, and they are following everything we said.

1 We've done two reports on it. As we've gotten more
2 comfortable with what they're doing and they have shown
3 their ability to actually comply with the requirements,
4 we're willing to give them a little more leeway, a little
5 more, and a little more.

6 Originally, they weren't allowed to have any PII
7 at all, even if the person was in Haiti under a building.
8 We were, no, we don't trust you with PII; you're not doing
9 that; that's not your authority. They've shown that and so
10 you see seven categories of PII that they're allowed to have
11 and do something with.

12 MS. CALLAHAN: And that's it. So the list is not
13 --

14 MS. RICHARDS: It's not one of them.

15 MS. CALLAHAN: Literally, public figures engaging
16 in public activities in the realm or individuals who have
17 engaged in a terrorist activity and that have subsequently
18 died.

19 MS. RICHARDS: Dead terrorists.

20 MS. CALLAHAN: Dead terrorists.

21 MS. RICHARDS: They have to be dead.

22 MS. CALLAHAN: The Fort Hood shooter is alive, but

1 the Virginia Tech shooter would have been an example of
2 somebody whose information could be monitored.

3 MS. RICHARDS: And the Arizona Rep who was shot
4 was a public figure in a public activity and she was
5 actually -- that actually occurred the day after we approved
6 them to have the PII and so they very responsibly reported
7 that, and we watched it very closely to make sure what they
8 were and weren't reporting. But that was a public figure in
9 a public situation, and so that was an appropriate use of
10 that.

11 MR. BEALES: Just so I understand what the state
12 is now, if I tweet that, help, I'm under a building in
13 Haiti.

14 MS. RICHARDS: We will come get you.

15 MR. BEALES: Oh, thank you.

16 (Laughter.)

17 MS. RICHARDS: That's the idea, yes.

18 MS. CALLAHAN: Howard, if you tweet that you're
19 under a building in Christchurch, New Zealand, OPS is
20 probably looking at related activities, related to
21 earthquakes. They would call New Zealand and say: Howard
22 is in the building underneath.

1 And Japan actually had a quake, 7.3. We got that
2 from our media monitoring while sitting in here.

3 CHAIRMAN PURCELL: Lance.

4 MR. LANCE HOFFMAN: Following up on what Howard
5 said, I'm interested in the flip side of it, which is, okay,
6 there's event number one and nothing bad happens and all the
7 information goes away, nothing, we're not worried about it.
8 Event number two happens and then something bad happens, and
9 so, as you described, it becomes a law enforcement event.
10 It goes to the FBI generically or whoever.

11 2 months later, event number 3 happens. Something
12 else bad happens at event number three. Who's connecting
13 the dots? Is it you? If it's not you, is it at least
14 somebody, or do we know?

15 MS. CALLAHAN: So let's be very clear. It is not
16 the DHS Privacy Office, okay. The DHS Privacy Office does a
17 lot of things, but we are not connecting the dots.

18 But it would be whoever's authority it is, and
19 most likely it would be an investigatory agency in the
20 federal government.

21 MR. LANCE HOFFMAN: So once it becomes a law
22 enforcement issue, the information gets -- does DHS --

1 MS. CALLAHAN: They have different authorities to
2 collect.

3 MR. LANCE HOFFMAN: But does the system shovel it
4 to them?

5 MS. CALLAHAN: So again, these narrow summaries of
6 information are basically alerts. They're breaking news
7 information. If the FBI looks at that and says that's
8 something that in my capacity we should investigate, then
9 they investigate and they do whatever they want. They may
10 have started with a kernel of the information from DHS, but
11 it is the investigatory agency's authorities and collection.

12 MR. LANCE HOFFMAN: They're alerts; they are not,
13 say, collections of data, pictures, whatever?

14 MS. CALLAHAN: No, no, no. They're just alerts.
15 They're really just alerts.

16 MR. LANCE HOFFMAN: Okay.

17 CHAIRMAN PURCELL: The bat signal.

18 Ramon.

19 MR. BARQUIN: I just want to -- again, there are
20 data sets that are duly protected separately by public law,
21 Census for example. The database of organ donors or organ
22 recipients, those kinds of things are sensitive, and they

1 are protected in some way.

2 What I'm trying to get is, right now I think
3 you've done an excellent job in establishing certain
4 guidelines so that what is currently being collected is
5 minimal, it probably applies totally within the FIPPS,
6 etcetera, etcetera, etcetera. But the question I think
7 where Lance is going and we'll eventually need to wrestle
8 with is, will there eventually be PII data collected through
9 these means -- and social media is what it's all about these
10 days -- that should in some way be protected above and
11 beyond, so that if the FBI or whoever needs to get hold of
12 it, it should go through a separate process, whether it's
13 judicial or not.

14 That was the only thing, just a comment, not a
15 question really.

16 CHAIRMAN PURCELL: That's fine, but we have to
17 remember that the provider of the social media service
18 itself has the most data, and law enforcement is going to go
19 to them first. Frankly, an FBI agent's not going to take
20 crappy little DHS OPS stuff and depend on it entirely.
21 They're going to go to -- it's an indicator and they would
22 go to the source for a much more fulsome situational

1 awareness and investigative thing.

2 So I guess the point is that somebody turns on the
3 recorders at some point, but it isn't DHS.

4 How are you feeling?

5 Eric, thank you very much for your testimony
6 today.

7 MR. LECKEY: Thank you.

8 CHAIRMAN PURCELL: We appreciate it. It was very,
9 very useful and very instructive. Thank you.

10 MR. LECKEY: Thank you.

11 (Applause.)

12 PUBLIC COMMENTS

13 CHAIRMAN PURCELL: We've come to the part of the
14 meeting where we are receiving public comments. We have had
15 one sign up for public comment, so I'll invite our person
16 who signed up. Ginger McCall, if you could step forward and
17 address the committee, we'd be happy to hear from you.

18 MS. CALLAHAN: Can I sit here?

19 CHAIRMAN PURCELL: Fine. Anywhere you want to be
20 is fine. We can hear you.

21 Welcome, Ginger. Ginger is the Staff Counsel and
22 Assistant Director for the Electronic Privacy Information

1 Center's Open Government Program; is that correct?

2 MS. McCALL: I actually have two questions. So
3 the first question has to do with the body scanner machines.
4 We've been doing a lot of work on that at EPIC and we had a
5 letter exchange with Mary Ellen about this. In the letter,
6 which I have right here with me, it seems as though what the
7 letter is saying is that DPIAC has somehow endorsed or
8 signed off on these machines. So my question is, have
9 you in fact done that?

10 My second question has to do with the FOIA
11 requests. I do a lot of work on FOIA in the course of an
12 average day, and we've noticed a kind of strange pattern
13 happening recently. I know Mary Ellen had said that they've
14 cleared a lot of FOIA requests, but we've started to receive
15 these letters, and the letters are a response to what is
16 usually a very clear FOIA request to the agency. The letter
17 says that if we don't clarify our request, our already very
18 clear request, in the next 20 days, that request is going to
19 be automatically administratively dismissed. So the request
20 will just cease to exist in the agency's systems.

21 I would like to know, are we getting a report on
22 how many of these reports that the agency claims to have

1 cleared have actually been cleared in that fashion, where it
2 seems completely illegal, what they're doing? There's no
3 allowance for this under the Freedom of Information Act. So
4 I'd like to know what percentage of those, quote unquote,
5 "cleared requests" have been cleared that way.

6 CHAIRMAN PURCELL: As an advisory committee, we
7 have no authority to approve or disapprove of any particular
8 technology deployment. We advise as to whether we think
9 it's a good idea and we advise as to whether we have
10 suggestions for improvements or enhancements. But for
11 better or worse, our authority doesn't extend to the fact of
12 actually stopping a program.

13 I'll invite Mary Ellen also to respond to that, as
14 well as Committee members, which I'm happy to do. David,
15 Jim?

16 MR. DAVID HOFFMAN: Can I just respond real
17 quickly?

18 CHAIRMAN PURCELL: Sure.

19 MR. DAVID HOFFMAN: I'm reading Mary Ellen's
20 letter here also and I -- I can read it again, but I think
21 everything that's stated in it is completely accurate, and I
22 don't believe that she uses the language "sign off" or

1 anything. We get briefings, we ask questions, we provide
2 guidance based on that. Based on my reading of this -- I
3 can go back and check on my notes -- I believe everything in
4 Mary Ellen's letter is perfectly accurate.

5 CHAIRMAN PURCELL: Jim?

6 MR. HARPER: I don't dispute the accuracy of the
7 letter, but I think it's important to consider as a
8 Committee whether this kind of letter is an appropriate use
9 of the Committee, because we are, like it or not -- and I
10 don't; it's a practice that precedes Mary Ellen -- we're
11 under a tasking order regime, where we don't speak as a
12 Committee unless we have a tasking order that has asked us
13 to speak.

14 So in that context, I don't think that holding out
15 the Committee as having reviewed and failed to object to
16 these machines is an appropriate use of the committee. So I
17 didn't find the letter -- again, I didn't find it
18 inaccurate, but I did find that it was -- I didn't think it
19 was an appropriate letter to send in the context of
20 defending this program.

21 So ask us to assess the program and take what you
22 want away from that, but don't not ask us to review the

1 program and then hold us out as having failed to object.
2 That's inconsistent with the tasking regime. If we want to
3 revisit tasking, I'd be happy to.

4 In the early years of the Committee, some of us
5 may remember, we would ask for stuff. The Privacy Office
6 staff would scurry happily around and produce witnesses that
7 -- one of them is back in the corner smiling -- produce
8 witnesses on subjects that were interesting to us, and we
9 would sua sponte come up with the subject matters we wanted
10 to address. I'd love to go back to that.

11 Right now, we're working apparently under tasking
12 orders that some of us haven't even seen, and it's getting a
13 little weird. I'd like to propose that perhaps tasking
14 orders should be put online so that everybody can see them
15 and they can distinguish between things that the Committee
16 did under a tasking order and things that the Committee
17 didn't do.

18 Right now I'm working in the transparency area on
19 legislation and my argument is that the goal should be that
20 a thing doesn't exist until it's online. The introduction
21 of a bill in Congress, I'm going to argue, and its
22 publication online should be the same thing. Maybe we

1 should lead in the transparency area by doing that with
2 tasking orders.

3 CHAIRMAN PURCELL: David, did you have a follow-up
4 to that?

5 MR. DAVID HOFFMAN: I just think we're getting
6 caught up in differences in language. And maybe, Ginger,
7 you can help with this. My understanding was that Mr.
8 Rotenberg sent in a request and wanted information back on
9 the degree to which the Committee had been briefed on AIT
10 and that that's what the letter sent by Ms. Callahan did.

11 That was my understanding of the letter exchange,
12 which is I think a bit different from Jim's understanding.
13 Maybe you could clarify exactly what Mr. Rotenberg was
14 looking for?

15 MS. McCALL: My understanding of it is that he was
16 asking for this Committee to review the technology.

17 CHAIRMAN PURCELL: If I may, the opening of the
18 letter states: "Pursuant to the Federal Advisory Committee
19 Act, I am writing to ask that you request the Department of
20 Homeland Security Data Privacy Integrity Advisory Committee
21 study the impact of the Transportation Security
22 Administration's airport body scanner program on

1 individuals' constitutional and statutory rights."

2 In other words, he's asking for a tasking. Fine.
3 We have -- so that's entirely different from a review or
4 approval or anything, any characterization like that. He's
5 asking, requesting for a tasking. That's the Privacy
6 Office's job to do that, and I think that's to -- to ask the
7 Committee questions. We've had lots of questions, lots of
8 opportunities to review. We haven't been tasked to study
9 the problem or write a paper about it.

10 Mary Ellen?

11 MS. CALLAHAN: I see there are plenty of questions
12 from the Committee members. Go ahead.

13 CHAIRMAN PURCELL: Fine.

14 Howard?

15 MR. BEALES: I just wanted to respond a little bit
16 to Jim's comments, because I think one of the other things
17 we do as a Committee is we get briefed in a public setting
18 about things that -- and I'm not sure that this was one of
19 them --

20 MS. CALLAHAN: It was, Howard.

21 MR. BEALES: It was, okay. But it's fair to say
22 this was out there. We were on notice. I don't think you

1 can draw -- I agree with you, you can't draw an inference
2 from the fact that we didn't object. But to say that this
3 was out there in public, we told the world that this was
4 coming, is a fair thing to do; and that we happened to be
5 the forum, as opposed to congressional testimony about this
6 that this was coming, doesn't bother me.

7 CHAIRMAN PURCELL: Dan? One moment, Jim.

8 MR. CAPRIO: Let me take a slightly different take
9 on this. I think that communications is always hard. It's
10 always difficult. We all get busy and communicating among
11 one another is time-consuming and it's always the last thing
12 that we do, even though our intention is to communicate.

13 So I think an issue worth considering going
14 forward -- there was a bit of a -- a heads up about that
15 letter would have, I think would have been appropriate. To
16 Jim's earlier point, I can't speak for the entire Committee,
17 but some of us found out about that letter in the media, and
18 it sure would have been nice to have had a heads up or some
19 sort of communication that it was at least coming down --

20 MS. CALLAHAN: Which letter? The EPIC letter or
21 the --

22 MR. CAPRIO: No, the response.

1 MS. CALLAHAN: The response.

2 MR. CAPRIO: The response. So it's just something
3 to consider going forward, because it's just never good to
4 be surprised with a public letter, as I know I was when it
5 was released.

6 CHAIRMAN PURCELL: John.

7 MR. SABO: Just a quick comment reinforcing the
8 points about tasking. That's been a standing practice.
9 But, having said that, we are the Data Privacy and Integrity
10 Advisory Committee, and I'm just giving you my personal
11 perspective. We're often asked to look at the use of
12 technology from a privacy and data integrity perspective and
13 to provide inputs on that. Sometimes it's more informal.
14 We were given a tour of the use of one of the technologies -
15 - what airport was that? -- and having seen the controls
16 that were put into place with respect to the actual on-site
17 use and the assurances that we were given about not
18 recording and not attaching the images to an individual
19 identity at that time, we evaluated those aspects of it and
20 we I think generally were -- we did not go ballistic, that
21 there were controls in place that separated the operator
22 from the individual, etcetera.

1 Now, that was not a tasking. We were just
2 reacting as individual members of the Committee, and I don't
3 recall that we were asked to as a Committee to put together
4 a finding. And that is the distinction, that a lot of our
5 work that is not visible to Mark and to other people who are
6 very concerned in the advocacy community about data privacy
7 -- that work is invisible, because we're providing a lot of
8 individual feedback as experts on this, but it doesn't
9 necessarily rise to the level of a tasking.

10 I just want to make that distinction, because we
11 did observe certain things. Some people were less, some
12 more comfortable with it. But in any event, controls were
13 put into place and we were given assurance, and that was the
14 basis on which I think -- I'm assuming, Mary Ellen -- in
15 addition to the public discussions, that's I'm assuming is
16 the nature of her points of the letter.

17 So I just wanted to make that. There is a
18 distinction between what we do in a very formal findings way
19 and what we do in our onsite inspections, etcetera.

20 CHAIRMAN PURCELL: Neville, did you have anything?

21 MR. PATTINSON: It was just to say pretty much
22 what John was going to say, which is that we had the

1 privilege to go and tour and visit under TSA's privacy
2 officer. Peter Pietra took us round that facility and the
3 privacy controls that were put in place were exceptional.

4 Now, we're not making any opinion on the machines
5 and the usage, but the operation of those machines and the
6 procedures in place to isolate people from certain parts of
7 the system while others were being submitted to the use of
8 the equipment were exceptional. And I don't think any of us
9 could fault the privacy controls that they'd thought about
10 very hard and put in place in protecting the information and
11 isolating components of that operation from each other.

12 I think it was an exceptionally good and well
13 thought out implementation. Now, is that conducted, unified
14 between all of the installations? I don't know. I visited
15 one facility. But if they're guilty of anything, it's not
16 publishing enough of the privacy protections they've put in
17 place, which are I think extremely good and effective.

18 CHAIRMAN PURCELL: Jim.

19 MR. HARPER: I think I agree with John and Neville
20 both that the DHS, TSA, and in particular Peter Pietra, the
21 TSA privacy officer, have done an incredible amount of work
22 to try to make this the least privacy-invasive it could be

1 in the context of a highly privacy-invasive technology.
2 It's a tough problem.

3 Actually, thinking on this, I said words to that
4 effect at a Heritage Foundation event and found a couple
5 months later that someone at Heritage was characterizing me
6 as having signed off on the technology and saying hooray.
7 No. They've done the best they could, and that's what I
8 said. So I took after that person for mischaracterizing my
9 views.

10 In my mind, this is an analogous situation, where
11 we looked, we appreciated the work that had been done, but I
12 don't want to be held out in the context of this
13 conversation for people who are not part of this Committee
14 and don't follow our Committee day over day. They read it
15 as DHS privacy committee's okay with it because we didn't
16 object.

17 It's also important to recognize that when we
18 looked at it that was a prior policy situation than the
19 present day or the current time for these letters, which is
20 where a person had the option of going through this machine
21 -- the option -- or getting a prison-style patdown search.
22 That was a new policy that came into place. So we're being

1 held out as endorsing an important part of that new policy
2 that we had nothing in mind about at the time we looked at
3 this technology. So again I think it was a careless use of
4 the Committee to speak about our having reviewed it.

5 CHAIRMAN PURCELL: And Joanne.

6 Ms. McNABB: I actually want to speak to the other
7 point, about the FOIA request, because I actually did have
8 the question in my mind when Mary Ellen was making the
9 report about that it would be useful to know the disposition
10 of all the cleared FOIA requests, how many of them were sent
11 back, we need more clarification, how many of them were
12 denied, how many of them were granted.

13 I'm in a place where I respond to that kind of
14 request at the state government level and I know that we do
15 track them in that way ourselves.

16 MS. McCALL: Yes, we'd really like to see that
17 information. The problem with this particular letter that
18 they're sending us isn't that it's a request for
19 clarification. That's fine. They're allowed to do that.
20 The problem is that if you don't respond within 20 days and
21 clarify what is already arguably a very clear FOIA request,
22 they'll just administratively dismiss it and pretend that

1 the request was never made. That does not have any sort of
2 standing under FOIA. There's nothing in the FOIA statute
3 that would excuse that kind of agency behavior.

4 MS. CALLAHAN: Maybe I could address both. At
5 this point I think all the committee has spoken on both
6 questions, so I thought perhaps I would address both of
7 them.

8 Ms. McNABB: Great.

9 MS. CALLAHAN: With regard to the request to have
10 an individual tasking, as you guys know, we have had several
11 -- detailed in the letter, we have had numerous public
12 briefings, in-person briefings, technology briefings, and
13 other discussions with regard to AIT from 2007 until the
14 present.

15 The privacy protections that were discussed in
16 abstract or in the initial concept in 2007 are the same
17 privacy protections that are in place in 2011. Therefore,
18 the thought of a tasking -- and as Neville points out and as
19 John points out, no additional privacy protections in all of
20 our discussions and public debates and online were -- no
21 additional privacy protections were identified. Therefore,
22 the concept of doing an individual tasking seemed to me to

1 be redundant, and the record was in the public domain, as it
2 has been for the past 4 years.

3 The letter I sent did not say that they have
4 signed off on it. They have not signed off on it. What
5 they have not done in several different fora in several
6 different states in several different years is identify any
7 additional privacy protections. Therefore I thought it did
8 not warrant the Committee's time, which is very precious, to
9 then have an additional tasking where they would go and say
10 there are no additional privacy protections that can be
11 considered.

12 So that is what the letter conveys. You can
13 represent it as conveying something else, but that is the
14 point of the letter, to say this is the fact, this is the
15 history, the fact that the protections have not changed
16 means that the precious time of this Committee does not
17 necessarily warrant working on that.

18 With regard to FOIA, absolutely those numbers are
19 available on my annual FOIA report. So if you look when
20 they say that there's no disposition on it, those are the
21 numbers where we've attempted to clarify. You may think
22 they're clear; we may think that they're not clear. And

1 that the letters that we have been using actually have been
2 in use since 2008 in terms of trying to resolve the issue
3 with a request that may be too broad and to try to narrow it
4 in scope. So those numbers are available in the annual
5 report, which was published January 19, 2011.

6 Thanks.

7 CHAIRMAN PURCELL: Thank you.

8 MS. SOTTO: May I ask a quick question?

9 CHAIRMAN PURCELL: Yes, please.

10 MS. SOTTO: Just a question for Mary Ellen. Is
11 there an appeals process with respect to clarity, in case
12 there's debate as to whether something is clear or not?

13 MS. CALLAHAN: Yes. So if you are dissatisfied
14 with the disposition of a FOIA -- and by the way, we don't
15 say that the FOIA never happened. It's just counted as
16 without resolution. So it is in our numbers.

17 If you're dissatisfied with the resolution, you
18 have two different options, one administrative and one
19 through the courts. The administrative appeals process is
20 coordinated by the Office of General Counsel, so again it's
21 an objective second party who is doing the review. Then
22 that administrative appeals process, that's what I was

1 talking about we had 2747 appeals that were pending. Those
2 have been knocked down significantly, thanks to the focus of
3 the appeals attorneys.

4 Or the other alternative is to go to court and to
5 seek clarification through the court system for an either
6 constructive denial, you don't get the records on time, for
7 again not satisfied with the disposition of the FOIA request
8 itself. So there are two different venues.

9 CHAIRMAN PURCELL: Can they be sought
10 sequentially?

11 MS. CALLAHAN: Yes, yes.

12 CHAIRMAN PURCELL: So one can go to the General
13 Counsel and, lacking satisfaction, continue and go to a
14 judicial process?

15 MS. CALLAHAN: Yes.

16 CHAIRMAN PURCELL: Okay.

17 MR. PIETRA: There's a reg that has all that.

18 CHAIRMAN PURCELL: Pardon?

19 MS. CALLAHAN: There's a regulation, 6 CFR 5, I
20 think.

21 CHAIRMAN PURCELL: Okay.

22 MS. CALLAHAN: But anyway, so there's a process

1 and it's a pretty straightforward process that all of the
2 departments follow.

3 MR. PIETRA: And that fits in the statutory grant
4 to the agencies to promulgate regulations implementing the
5 FOIA statute. So there is actually a legal basis for the
6 process.

7 MS. McCALL: Is this the basis that you used to
8 say that you can administratively dismiss these FOIA
9 requests after 20 days if there isn't clarification?

10 MS. CALLAHAN: The FOIA -- and I think we need to
11 wrap up pretty soon, Mr. Chairman --

12 CHAIRMAN PURCELL: Yes.

13 MS. CALLAHAN: I think, because I believe, Ms.
14 McCall, you had 3 minutes.

15 The FOIA provides that the request has to be
16 clear. It has to be that you're seeking records, and if the
17 records are not able to be identified then the FOIA cannot
18 be processed. That's the type -- that's why we're
19 attempting to communicate with requesters if indeed the
20 request is not clear. Actually, I think it behooves all of
21 us and it's good government to go and make sure that we
22 understand what you're asking for, what you'd like to

1 prioritize, and how you'd like the records to be
2 transmitted.

3 MS. McCALL: Now, when I called DHS about that and
4 did get in touch with a person, I was told by that person
5 that in fact there was nothing wrong with my FOIA request, I
6 didn't need to worry about that clarification, and the
7 request was later fulfilled as written by us originally.

8 CHAIRMAN PURCELL: Well, this is a FOIA issue
9 specifically that I'm not sure if you're seeking relief or
10 --

11 MS. McCALL: I'm not seeking relief. My question
12 --

13 CHAIRMAN PURCELL: -- putting it on the record.

14 MS. McCALL: My question was simply we would like
15 to have the numbers.

16 MS. CALLAHAN: They are provided. They were
17 provided in the 2011.

18 MS. McCALL: The question was where could we find
19 those numbers, and to call to this Committee's attention the
20 fact that these letters are being sent out and we feel that
21 they have no basis under FOIA.

22 MS. CALLAHAN: Consistent with FOIA. Consistent

1 with FOIA 5 USC 552, as well as the regulations, as Peter
2 points out, as well as published DHS policy.

3 I think, Mr. Chairman --

4 CHAIRMAN PURCELL: Closing. Thank you very much
5 for your inquiry and your question.

6 Are you going to make one last comment here?

7 MR. HARPER: I just did, yes. Back on the letter
8 issue, I wonder, Mary Ellen, if you could -- you would agree
9 to put on the DHS committee web page that we are subject to
10 tasking orders.

11 MS. CALLAHAN: It is on the page.

12 MR. HARPER: And to publish the tasking orders
13 that we have had in the past and that we have presently.

14 MS. CALLAHAN: That's a great recommendation, Jim.
15 We already do that. The charter is available online and the
16 tasking letters are also online.

17 MR. HARPER: I'll look for the tasking letter I'm
18 currently working on, which I have not seen.

19 MS. CALLAHAN: Great.

20 CHAIRMAN PURCELL: Thank you very much for your
21 inquiry and comment, Ms. McCall. I appreciate it.

22 Lacking any other sign-ups for public comment, we

1 call this meeting to an end and adjourn. Thank you very
2 much for your participation.

3 (Whereupon, at 4:29 p.m., the meeting was
4 adjourned.)

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22