DEPARTMENT OF HOMELAND SECURITY

Data Privacy and Integrity Advisory Committee

Washington, D.C.

Thursday, May 14, 2009

A T T E N D A N C E

Acting Sponsor:

Mary Ellen Callahan, DHS Chief Privacy Officer

Executive Director:

Martha K. Landesberg, Associate Director,

Privacy Policy and Education, DHS Privacy Policy

Members:

Joseph Alhadeff

Ana I. Anton

Ramon Barquin

J. Howard Beales III

Thomas M. Boyd

Daniel W. Caprio, Jr.

Renard Francois

D. Reed Freeman, Jr.

Kirk Herath

David A. Hoffman

Lance Hoffman

Joanne McNabb

Charles Palmer

Neville Pattinson

John Sabo

P R O C E E D I N G S

MS. LANDESBERG: Good morning, everyone, and welcome to the May 14th, 2009, meeting of the DHS Data Privacy and Integrity Advisory Committee. I welcome you. I am Martha Landesberg, Executive Director of the Committee and Designated Federal Official for the Advisory Committee.

I'll now turn the meeting over to Chairman Howard Beales.

MR. BEALES: Thank you, Martha, and welcome, everyone, to our public meeting today. If I could ask that you please be sure and silence your cell phones, we would greatly appreciate it.

Also, we have reserved time for public comments from 3:30 to 4:00 at the end of our agenda. If you are interested in addressing the Committee then, please sign up at the table that's outside the room, and we would be happy to hear from you.

I'd also like to say as we begin this meeting, this will be my last meeting as Chair. I have really enjoyed the privilege of being your fearless leader for the last couple of years, and I think now that we have a new Chief Privacy Officer who is with us today for the first

time, it is appropriate for her to name a new Chair. I look forward to continuing to work with you as a member of the Committee and hold up my tent with the rest of you, as opposed to hogging the microphone.

With us today we do have Mary Ellen Callahan, who is the Chief Privacy Officer. She became the Chief Privacy Officer on March 9th, and we are -- we welcome you and we are very pleased to see you.

Prior to joining DHS, she specialized in privacy, data security, and consumer protection law as a Partner at Hogan and Hartson. She worked there for more than 10 years. She was the Co-Chair of the Online Privacy Alliance and the Vice-Chair of the ABA's Anti-Trust Division, Privacy and Information Security Committee.

She holds a J.D. from the University of Chicago Law School, a fine school, and graduated magna cum laude from the University of Pittsburgh. Before law school, she worked at the Congressional Research Service of the Library of Congress as part of a special task force on the development of parliamentary institutions in Eastern Europe.

Mary Ellen, welcome. We look forward to

hearing what you have in mind for the Privacy Office.

DHS PRIVACY OFFICE UPDATE

MS. CALLAHAN: Thank you very much, Howard, and thank you for your fine leadership over the years.

Howard and, as I'm going to discuss later, Howard and Lisa have served over 15 months past their time as Chairman and Vice-Chairman, and I'll discuss some of my ideas or thoughts about transition. But I wanted to thank Howard for continuing to serve as Chairman well beyond the time that he was initially asked to do so, and we're thrilled that he's going to continue on the Committee until 2011.

I want to welcome all of you. I'm thrilled to be here. I'm very excited to work with this Committee on advice and collaboration regarding the Department of Homeland Security. This is my first time appearing before the Committee.

I also want to wish a special happy birthday to Reed Freeman, who, amazingly, actually ages. Can you believe that?

[Laughter.]

MS. CALLAHAN: So happy birthday, Reed. Thanks for spending it with us.

I want to give you updates on what the Privacy Office has been doing since we last met on February 26th, when I appeared as an observer. And I also want to share, as Howard mentioned, my thoughts about the Committee's strategic vision for this year and going forward. And I want to, of course, thank you all for your best wishes and for your continuing support of the Privacy Office and of the Department of Homeland Security.

With regard to today's meeting, consistent with what I have spoken with all of you about, consistent with my theme for 2009, which I'll discuss in greater detail, this morning the Committee will hear a presentation from US-VISIT with regard to their redress program. In addition, the E-Verify program staff will also update the Committee on steps taken in response to the Committee's 2008 recommendations on employer verification and other recent developments.

And I also look forward to the Committee's deliberations this afternoon on the Data Acquisition and Use Subcommittee's white paper on Information Sharing and Access Agreements. I would like to particularly thank the Subcommittee and its leaders for their intensive work on

the document, and should the Committee approve it, I believe the white paper could have a significant impact on how the Department conducts its information sharing agreements. So I want to thank you for that.

Just a little bit of background and general observations. It's been a whirlwind, as I was discussing with people earlier, but a great opportunity for me since I took over in early March. And as usual, there's a lot to report and, in fact, maybe even a little more to report than usually takes place. So please bear with me as I let you know the detailed and expansive work that my office is doing. And as you know, my office really is a phenomenal group of individuals and a great collective. And so I'm really thrilled to be working with them on privacy issues here in the Department.

The first area I want to discuss is compliance and our compliance team. It is really kind of the meat and potatoes of the office. It is where we do most of the kind of public-facing work, including the Privacy Impact Assessments, System of Records Notices, and also work with the other components with their Privacy Officers and their privacy teams to make sure that we have an accurate

description of the privacy impacts of DHS technologies and programs.

A few things that the compliance team has done since we last met. As required by Section 803 of the 9/11 Act, we recently published our second quarterly report to Congress on the privacy reviews and guidance. A copy of that is available in your materials. It also, I believe, was distributed to the DPIAC and, of course, is made publicly available, and I believe there are copies outside.

In addition, we are doing a biennial review of all of our System of Records Notices, the SORNs, beginning with those that were not reviewed during the legacy update project completed late last year, and we plan to schedule all 130 SORNs for biennial review beginning in September so we can systematize this and to make sure that the System of Records Notices are accurate, and to republish them as necessary to make sure, now that we've done a comprehensive review of what's currently on the books, we're going to make sure that we continue to make sure that they're accurate.

The compliance team is reviewing public comments on 35 different DHS Notices of Proposed

Rulemaking where Privacy Act exemptions are sought, and we're working on finalizing the final rules in that capacity.

Of course, this team also provides training, and it does so periodically throughout the Department on Privacy Impact Assessments and SORNs, and this year's annual workshop, which is open to all Federal employees and contractors, is June 10th here in Washington, D.C., so mark your calendars.

As part of my review of the Office, as I think I've mentioned to some of you, I'm considering revising the PIA form, but not the substance. I just want to make sure that the analysis and the issues are appropriately highlighted, and I'll welcome input of the Committee on that issue.

As you are well aware, there's been considerable public discussion of DHS analytical products. There is now an interim directive from the Secretary and Deputy Secretary that the Privacy Office and the Office of Civil Rights and Civil Liberties review all I&A analytical products. This is a heavy lift for a relatively small office, but quite frankly it's a great opportunity for the

Office and a great signal on behalf of the Secretary and Deputy Secretary.

We're reviewing the analytical I&A products to ensure all information is within and consistent with privacy requirements, and we're working with I&A to ensure that all parties understand the boundaries of information requests made, for example, to fusion centers and to others.

With regard to policy, that, of course, is a very active area for our office. The Office, under the leadership of Toby Levin, has been working to extend our already formidable influence on interagency privacy efforts, which have been intensified as a result of President Obama's Memorandum on Transparency and Open Government.

In keeping with our leadership role in cutting-edge privacy issues, we are also holding a public workshop on government use of social media on June 22nd and 23rd, again here in D.C. The Policy and Privacy Technology and Intelligence teams have been taking the lead on this, and we're really excited about this conference. We think it's going to be really a signature piece in terms of the

confluence of legal, policy, and technology security issues associated with government use of social media. We're going to have demonstrations of Federal websites. We're going to have discussions on the privacy impacts. We're going to have hopefully key policymakers also giving their vision of government use of social media, which of course is part of the President's Open and Transparent Government Initiative. And government use comes with some complications that we hope to note and address relatively quickly. We'll be issuing a report after the workshop.

In addition, I have been appointed one of the Co-Chairs of the Federal CIO Council's Privacy Committee, which is an interagency committee dealing with privacy issues. With me in that role, and previously we did not have a Co-Chair position, it gives us a lead role in developing guidance with, for example, OMB on privacy education and best practices in the Federal Government, along with, as I've noted earlier, the current focus on government use of social media.

The policy team is also developing privacy training materials for state and local fusion centers and

for DHS staff assigned to those centers. And as required by the 9/11 Act, as you may recall, we're beginning our annual review of the Department's data mining activities early this summer, and we'll issue our report in December.

The Privacy Technology and Intelligence Group also has been quite active. Our Office continues to work to build privacy protection into, for example, the Federal government's cybersecurity efforts.

Our team has been providing support to the White House's 60-day Review of Federal Plans, Programs and Activities to protect Federal computers. They did so by, for example, coordinating privacy advocates' input into the review process.

In addition to our ongoing review of DHS systems generally for privacy issues, our Privacy Technology and Policy teams have been working with the DHS Science and Technology Directive on a plan to implement the privacy principles for S&T research projects that we first announced in last year's data mining report, to make sure we get some concrete examples of how to implement those principles in the science and technology arena.

In this area, I've also been named a Co-Chair

of the Information Sharing Environment Privacy Guidelines Committee. The DHS Chief Privacy Officer was added as one of the three Co-Chairs, along with my colleagues at ODNI and the Department of Justice. This addition of me on the Privacy Guidelines Committee, which was first requested by my predecessor, Hugo Teufel, demonstrates the role that DHS and the DHS Privacy Office play in the Federal information sharing environment. So I'm quite pleased with that, and I thank Hugo for taking the lead on that.

With regard to the Freedom of Information Act, you heard from my colleague, Bill Holzerland, last time about what we're doing with FOIA. And as you know, the President's January memorandum on the Freedom of Information Act and Attorney General Holder's guidance on FOIA have generated a lot of public interest in government generally and in DHS activities in particular. And, quite frankly, I'm really excited about this because the Open Government and Transparency in Government Initiative is certainly consistent with the vision of this Office, both on the privacy side and on the FOIA side. And as a result, our FOIA team has been working intensively in trying to respond to the public's increased focus on FOIA

opportunities.

In addition, I'm working with the FOIA team to design a complete strategy about how DHS can proactively meet the President's initiative. So I look forward to reporting on that in our next meeting.

We, of course, now have a Privacy incidents and Inquiries team, and they are continuing to develop several new initiatives, one of which is the Electronic Complaint Tracking System which will address privacy complaints and respond to privacy access requests, and provide redress, as appropriate. This is an important team with regard to my vision for 2009 and the assistance that the Committee can provide.

The compliance staff is working with the inquiry staff to make sure the PIA and SORN are appropriate, and we hope to publish those and go live in July. We, too, must meet the same standards of compliance as the rest of the Department does when we have systems.

And then other efforts related to privacy incidents that are ongoing are with relation to the DHS Security Operations Center incident response team. We're trying to see that the privacy incidents are properly

reported to the Department and the components, and that mitigation and remediation efforts are appropriate for each incident. We're analyzing statistics to determine where incidents are occurring, targeting vulnerabilities, and working on training to prevent this from happening in the first place. And we are also revising our Handbook on Safeguarding Sensitive PII to even more effectively convey the importance of preventing privacy incidents and to reinforce incident handling and reporting procedures.

All of those things that I just mentioned are about the only thing that I did in the outside world that I'm doing in the inside world. But with that said, it's been exciting to work on a lot of different issues.

One area that I think I mentioned to you that I didn't expect to be as active in but certainly with the leadership of our International Privacy Policy group, is the international privacy work and the international outreach. The IPP group continues to follow international privacy policy developments mainly in Europe, and to provide support to DHS leadership. As Lauren and Shannon had explained to you last time, it's been quite busy in the international privacy discussion area.

Last month, Deputy Chief Privacy Officer John Kropf and I traveled to Paris, Berlin, and Brussels at the Secretary's request to foster U.S. and European privacy and security relationships. During that trip we met with the Ministers of Interior and Justice in each country to learn how our counterpart agencies provide privacy protections, and to explain the U.S. privacy framework and redress options for non-U.S. persons.

In my opinion, the meetings were extremely valuable, and also were helpful for gauging the stakeholders' interest in the success of the High-Level Contact Group since, of course, these communications were at the bilateral level.

In addition, during our trip we were able to meet with the EU Council and the Commission, and I believe that our future interactions with the Europeans will be very positive and mutually beneficial.

Other things that the IPP group has been working on, they too have been quite busy. In March, IPP staff participated in the OECD "Working Party on Information Security and Privacy: A Global Dialogue," which is a result of a paper and conference to assess the OEC

guidelines in 2010, which I might note marks the 30th anniversary of the OEC guidelines, kind of the grandfather of international privacy guidelines. So maybe we'll have a cake for them, just like we're going to have a cake for Reed.

Reed, we're not going to have a cake for you. I forgot, really.

[Laughter.]

MS. CALLAHAN: Sorry about that.

In addition, other international stuff that's going on. In fact, just this week, Tuesday perhaps, staff spoke on cybersecurity and privacy issues at the Max Planck Institute for Foreign and International Criminal Laws: Current Issues on IT. I have no idea what that acronym is, but I bet it's really long.

It was in Freiburg, Germany, and then we took the opportunity to meet with the Council of Europe's officials in Strasbourg to learn more about the Council's data protection initiatives, and we'll have more information on that in our next meeting.

We also, as you may be aware, are participating in exchange programs with data protection Freedom of

Information Act officers and other privacy offices throughout the world, and I think that that's been quite an effective mechanism and tool that we are going to continue. We just recently hosted representatives from the UK ICO and Mexico's Federal Institute for Access to Public Information, to gain greater insight into the respective privacy policies and programs. The week-long meeting included visits with, of course, our Privacy Office team, our DHS Office of Civil Rights and Civil Liberties, our component Privacy Officers, several of whom are here today, as well as others within the Federal Government, and we look forward to hosting additional ones in the future.

The final note on international. I just want to note that my Deputy Chief Privacy Officer, John Kropf, now Co-Chairs the CIO Council's Privacy Committee's new International Privacy Subcommittee, and we look forward to his work on that.

As you can tell by all of this information, we're pretty busy, and actually we're incredibly busy and we have a lot on our plate, but as I said, I think it's a great opportunity for the Office and for the Department.

And the good news is, to continue to support our mission, we actually have several -- we are recruiting several positions in our office, which I'm really excited about. We are -- we currently are posting for a Senior Privacy Analyst to work directly with John and me on policy issues. We also are looking for a new Associate Director of Privacy Compliance, as well as three entry-level Privacy Analysts who will work on domestic and international issues.

We have also created a new job, an Associate Director for Communications, whose job will be to help develop training materials and to promote a culture of privacy within the Department, and to develop a comprehensive privacy outreach program.

For example, this vacancy announcement closed on April 22nd, and we received over 300 applications. I think all of these are great signs. I'm really excited about all of these openings, and they're consistent with my theme, which I haven't talked about yet but I keep foreshadowing.

We also are hiring a Senior Attorney advisor who will work in the Office of General Counsel but will be focused on Privacy Act and FOIA opportunities, and I'm

really excited about this because we have not had a full-time attorney assisting us on legal issues for several years, and the previous one, although outstanding, was also on detail. So this is another great opportunity for us to solidify our role and to get the legal support that we need on the privacy and FOIA issues within the government, because as you may be aware, although I practiced, as Howard said, at Hogan and Hartson, I don't practice as an attorney in my role as Chief Privacy Officer.

Finally, on the hiring initiatives, as I said, I'm very excited about all of these different opportunities, and please encourage friends and family to apply. But there's one bittersweet note, which is the Associate Director for Privacy Compliance position is open because Nathan Coleman, who has served in that role and has been Acting Director of Privacy Compliance while Becky Richards has been on maternity leave, has taken a new job at the TSA in their legal counsel's office. It's a great opportunity for Nathan, and we're really excited for him. We will continue to work with him, of course, because of the TSA issues and outreach. But I wanted to publicly thank Nathan for all of his hard work, and we will indeed

miss him.

So I keep talking about my vision and my theme and what I'm thinking of for 2009. And now that you've heard all the things that we're doing, perhaps my theme makes a little more sense, which is the -- of course, the Office, as I said, is really a signature Federal Privacy Office, and the influence hopefully extends far and wide on issues as well as on policy.

That said, I think we can do more. I know we can do more. And it's with that goal in mind that I really hope to enhance the efficiency and the influence of the Privacy Office within the Department, first within the Department and then within the Federal Government.

As I have mentioned before, I think it's important to make sure that privacy and privacy protection are part of the analysis for all programs that take place in the Department, and that discussion should take place systematized throughout the Department within the components. It should be a matter of course, and we've been very successful on that in several arenas, but I hope to be 100 percent successful in terms of making sure that privacy is one of the calculations that takes place and

that we are always part of the discussion.

As part of this attempt to systematize privacy, we, of course -- privacy deals with individuals and with the public, and that's where the Committee comes in. I am so fortunate and the Office is so fortunate to have such an amazingly rich group of experts and wide range of experience on this Advisory Committee. And, quite frankly, we'd be remiss if we didn't capitalize on that. And with that said, what I would like to ask the Committee to do for 2009 is, building on the President's Memorandum on Transparency and Open Government, I would like this Committee to help us focus on those issues and to help focus on providing guidance on how to improve the Department's engagement with the public.

I mean that in several ways. I would like to seek your input and insights in how to effectively educate the public about individual rights and responsibilities with regard to Department programs; how to effectively convey the messages of privacy and privacy protection to the public; how to best provide individual access to data, to have the data corrected within our system; and how to provide effective redress when redress is called for.

As I mentioned, my colleague from US-VISIT is going to speak in a few minutes, and I would like to thank him because he forewent a very important meeting to be here with us today. So thank you, Paul. But I think that that will be a useful snapshot for you guys to hear how US-VISIT provides redress, but also then we can work following this meeting on how to define and refine some of the ideas that I have for The Committee.

In the near future I will work with you on assigning specific tasks that would reflect the theme of public engagement, but at the same time I decided to not define it prior to this Committee meeting because I wanted first for you to hear from Paul, also for you to hear from our E-Verify colleagues, who have a similar theme, and then together perhaps we can work on ideas to help move this theory and theme of engagement with the public forward.

And I want to talk a little bit about the Committee. As I said, this will be our theme, and I will work on working collaboratively to make sure that we have an effective vision for 2009.

I have also, in all of my individual

conversations with you, heard your commitment to making substantive contributions to the Department, and for that I greatly thank you. With that said, I would also like to work on making the Committee more effective and more efficient. And so, as Howard mentioned, I am greatly thankful for his fine work and for Lisa's fine work as the Chair and the Vice-Chair. I am also going to be, following this meeting, soliciting either recommendations or volunteers to take over the role of Chair.

What I'm thinking is that we'll have a new Chair in place by September. We may or may not have a role of Vice-Chair to take place as of September. Perhaps I'll wait until December, when hopefully we'll have the new additions to the Committee. As you know, we have solicited for applications, or re-applications in your case, for Committee membership for the 2009 group of people and the 2010 group of people, and that is currently ongoing, and I encourage all of you to reapply and to explain to me, as a relative newcomer, what you can help the Committee with, and I really welcome that input.

As you know from the materials that Martha has sent and from the Federal Register notice, the submission

materials are a cover letter and a resume. But I'd really love to know your vision in the cover letter. That would be very useful for me.

And so that application is due on June 8. So I encourage you to apply, and for those in the audience who are interested in applying, I also encourage you to apply. We are looking for diversity in experience and expertise and in industry. As you know from the Federal Register notice, we are, according to our charter, obligated to make sure that we have a wide range of complementary skills, including skills from academia, from non-profit, from the business community, including small and medium-sized businesses. With that said, the most important thing is to make sure that we've got experience, expertise, and enthusiastic participation.

So just to be clear in terms of the chairmanship, and I've spoken to Lisa about this as well, if you're interested in being Chair or you have an idea about who would be a good Chair, please let me know. I didn't want to nominate somebody before this meeting because I didn't know how much -- I know how much work it was for Howard, and I don't want to task someone to do it

if they don't think that they have the ability to do so. So I welcome the suggestions from the Committee.

I also, based on your observations, intend to work with Committee leadership and with the -- and I include in that the Subcommittees, to help revisit the Subcommittee structure, and I will ask the Subcommittee Chairs to convene their membership at least monthly. I think even with working on the taskings, you'll be meeting more than that telephonically. But to make sure that the work moves forward smoothly and collaboratively.

And I'm really excited about this. I expect this to be a very productive year for the Committee to provide true benefit to the Department and to our Office, and hopefully to me personally as well.

I encourage you to continue our dialogue, reach out to the Executive Director, Martha Landesberg. Feel free to contact me if you have questions.

At this time, I'm available for questions, Mr. Chairman.

MR. BEALES: Thank you very much.

Are there questions from members of the Committee?

John Sabo?

MR. SABO: Just a comment. It's great to have you on board as the Privacy Officer and hear some of the comments you've had about change and improvement.

I just wanted to comment on one aspect of one thing you talked about, and that was included in your vision, the focus on individual access. And I think that's really critical because individual access, by implication, means the ability to know where the information has actually flowed, and certainly the ability to correct and update as necessary, or dispute, which then of course leads into redress, and I think that's been a particular problem because systems move PI and PII all over the known universe, application after application, multiple agencies. And although I think there are technical approaches to that, it's a difficult issue to come in after the fact and begin architecting solutions.

So I think I just wanted to reinforce I think that's an important focus area. And even in the FIPPs policy statement, individual access is essentially tucked under individual participation. But frankly, my own view is that it's an equally important principle and practice,

and it's great to see you're elevating it in your attention. Thank you.

MS. CALLAHAN: Thanks, John. And I completely agree. You're coming at it, of course, from more of a technologist's approach than I would. But I think it's important to have both the technology, the application, and the policy all meet up in terms of access and really, quite frankly, data control.

MR. BEALES: Joanne McNabb?

MS. MCNABB: Thank you. Thank you, Mary Ellen. That was really interesting.

I would like to know more, and maybe this isn't the time, maybe it's at another meeting, about how the Office is working on the cybersecurity initiative, because we've been trying to do -- build some privacy considerations into efforts in California and finding it's kind of tough. It's new concepts to the people working in that area.

MS. CALLAHAN: I think we may have to table that for later consideration. What I can say is the Office and the issues of privacy and civil liberties were considered throughout the 60-day review, and quite frankly

it was very encouraging for me as a privacy person. I don't know what the final result is going to be, but we were definitely part of the conversation, which I think is a first step, as you point out, Joanne. And I can't tell you, as I said, what the final result will be.

With that said, I'm cautiously optimistic that privacy will be part of the conversation there. But perhaps we can table that until September.

MR. BEALES: Reed Freeman?

MR. FREEMAN: Mary Ellen, I had two choices. I went left.

[Laughter.]

MR. FREEMAN: So I just wanted to say something entirely procedural, which is to thank Howard for truly, truly great leadership. Under times where there has been confusion, maybe difficulties working through issues, Howard has, behind the scenes, been a clear voice, a steady voice, a calm voice to move things forward and produce work product that is analytically sound and has, in my view, been quite useful. So really, thank you, Howard.

[Applause.]

MR. BEALES: Thank you. You all made it easy.

MR. FREEMAN: Not always.

[Laughter.]

MR. FREEMAN: The other thing I wanted to say on a procedural note is to thank you for choosing to serve, Mary Ellen. It's not -- it's easy to think it might be fun. It's hard to undertake the enormity of the job and to expand it, and I want to congratulate DHS on landing this candidate because, in my view, and after some period of time, it's a relatively small group of people that play in this sandbox. I don't think there is a smarter, more clear-thinking, pleasant and hard-working person in the United States for this job, and I'm pleased that you took it, and I look forward to working with you.

[Applause.]

MS. CALLAHAN: Thanks, birthday boy.

[Laughter.]

MS. CALLAHAN: No, and I echo Reed's comments to Howard. I really do thank you for helping shepherd this Committee, and it's really been yeoman's work, as they say. And thank you, Reed.

This is really an exciting opportunity for the Department and for me personally. I was speaking with

Charles and Lance earlier, and I said I was just starting to have fun about 10 days ago. Before I was kind of like I don't know what's going on, and it's really interesting, and it's really exciting, and it's an exciting opportunity even on the cyber stuff and so on. It's really an exciting time, and I'm thrilled to serve, and I thank the Secretary.

MR. BEALES: Kirk Herath?

MR. HERATH: Thank you. Thank you for serving.

I guess I have a -- so you mentioned one of the things briefly. First of all, these are -- we were talking in our Subcommittee meetings yesterday about sort of where do we go from here, and we said we really can't decide until you lay out your themes.

One of the things that I am personally involved in and interested in is the whole incident management and response program. So I know that you have capabilities, and it seems to me, now having done this for about a decade, that you can tell a lot about the maturity and the integration and collaboration of the privacy function which seems to be at the center of most organizations' incident management programs.

Can we get at some future time an explanation

of that? Because I think that that really -- if you're going to talk about your efficiency, your integration and your collaboration, that really is -- shows a lot of transparency around whether you're doing it well. And it should be rule based. It should be a process that is both simple and complex, and obviously always going to the root cause, root cause, trying to prevent harm from people.

So that's something I think that I personally would like to help you with, and I think it goes with a lot of these other themes as well.

MS. CALLAHAN: I think that's a great idea, Kirk, and we'll definitely look into that for a future Committee, and perhaps work on the tasking. But I think it might be more appropriate in the Committee setting. So thank you for that suggestion.

MR. BEALES: Dan Caprio?

MR. CAPRIO: Thanks, Howard. And thanks, Mary Ellen, for your leadership and your willingness to serve. I appreciate your vision as you laid it out, and the President's vision for transparency and open government and the notion of improving public engagement.

But I'd like to pick up on Joanne's point

related to cybersecurity and the 60-day review. I have an understanding that the final decision hasn't been made, and obviously we can't talk about it. But I think once a decision is made, given the gravity of the situation and the national and economic security implications of cyber security, that it really would -- I think this has been a discussion item of the Committee for some time. But to the extent that we can be involved in terms of the privacy and civil liberties aspect and the public engagement of explaining to the public sort of what it is, why we're doing it, and reassure the public, whether it's civil society, industry, et cetera, of sort of what the government is doing and the notion of privacy and security.

So much of it, I'm sure, will continue to be classified. But to the extent that there is unclassified information where we can engage the public, I think I'd like to be part of it, but I think there are many others that would be willing to serve with you in that public engagement.

MS. CALLAHAN: And thank you, Dan, for that offer and for that suggestion. Quite frankly, I think that would be great, and I think that once the President has

made his final decision and how this goes, I think we would need the Committee's support. So we will come back to you hopefully in the near future with some kind of follow-up on that issue.

But I think it's hopefully consistent with my theme as well. I don't want to get too far afield in terms of the different issues, but I think that that certainly is part of the concepts of engagement and education. So, I say stand by.

MR. BEALES: Neville Pattinson?

MR. PATTINSON: Mary Ellen, congratulations on your appointment. Nice to meet you in person for the first time.

I'd like to pick up a theme, one of the themes that you mentioned in your mission, which I think is very admirable, engagement with the public. I think that's a terrific challenge. Understanding that you're looking to recruit an Assistant Director for Communications, I think that's going to be an essential role to help support that. Obviously, engaging the public requires resources, and resources will be busy dealing with questions, answers, and so on that are going to be coming in.

That shouldn't be underestimated. I think we've seen very good efforts by several components in engaging with the public already to date. The US-VISIT team has been really outstanding in their pushing of information out to individuals, TSA, and E-Verify. Those are three that I've just written down very quickly from notable experience and understanding. There are good examples of how information can be pushed out, rights can be explained, and information is given.

But I think this is something that you could capitalize on in the use of the social media activities that you mentioned at the beginning. This is an area which is proven to reach out to mass individuals, and that itself presents challenges, how do you control that information, how do we maintain privacy and anonym -- well, maybe not anonymity, but certainly confidentiality in that process.

So I think, understanding your vision and your theme and one of your objectives there, I think the social media outreach could be a very valuable tool in helping to manage that resource and to provide that reaching out to the public. So I sort of look forward to kind of stitching all those together.

MS. CALLAHAN: Well, thank you, Neville. And I, actually -- I, too, look forward to stitching all those together. For those of you who knew me in my prior life at Hogan and Hartson, you know I worked on social media for the past several years, and it was funny. When I came in, I was kind of like, ah, I know all the answers on social media. And then all of a sudden you put the Privacy Act on top of it, and you put the First Amendment on top of it, and you have all of these issues that really make it much more complex.

With that said, Neville, I completely agree that social media needs to be part of the conversation. I've got a really great team that's working on trying to figure out the legal issues, the policy issues, as well as the practical, and, quite frankly, safety and security issues in terms of protecting our infrastructure, and that's being led by Rosalind Kennedy, who is one of our technologists, as well as Toby Levin. We're working both within DHS on a task force in terms of defining it, and I think there have been some very good examples of good messaging out there.

And in addition, in the Privacy Committee I

mentioned, there is -- that's being led on the -- interagency-wide by Jonathan Cantor from Social Security, who is an outstanding Privacy Officer, and some of the legal support is being provided by Kirsten Moncada from the Department of Justice, to try to figure out how do we deal with these issues and comply with the President's directive for openness and transparency, that the President specifically said use social media, and people are using it, and I think we just need to make sure that they use it properly.

But I cannot agree more that this is really one way that we have to do it. We just want to make sure that we're doing it properly and efficiently. So I actually hope -- I think that's going to be hopefully resolved in short order. I mean, we may even be able to talk about that in September in terms of some of the decision points that have been made.

MR. BEALES: Ramon Barquin?

DR. BARQUIN: Like everyone else, Mary Ellen, thanks for being here.

I was just curious. We had put together a series of thoughts and suggestions that we had passed on to

the transition team, and now that actually the transition is sort of over, I'm just curious where did any of those land?

MS. CALLAHAN: Great. Thanks for that question, Ramon. I'm sorry I did forget to mention that. Howard, on behalf of the Committee, did write to the Secretary and to John as Acting Deputy -- Acting Chief Privacy Officer on, I believe, February 2nd with a series of observations, recommendations, and thoughts.

The Secretary has passed that on to me and has asked me to inform -- use this to inform my work within the Department this year, and there were 16 suggestions. Some of the suggestions have become moot because of how time has passed by. Some of them I'm working on now, and I think I have mentioned on phone calls to you not yet ready for prime time, but we're working on implementing some of the recommendations. And some of them were more kind of bigger picture themes where there's no tasking.

But it's certainly part of the things that I'm considering in addressing the Office, and it certainly is -- I understand the priority nature of the items in there. So it absolutely is informing me as I go forward.

MR. BEALES: Ana Anton?

DR. ANTON: Thank you very much for taking the position, and I think you've really shown us very early on that you're extremely enthusiastic, extremely competent, definitely very professional, and have a clear vision, and for that we're all very excited.

There are three themes, or two in particular, actually, that you touched on. We mentioned earlier -- Neville mentioned the social media. And so earlier in your comments, you spoke about the government use of social media. And so I was interested in knowing whether you see this as a mechanism to support government processes and/or as a mechanism for public outreach. So that was the first note.

Secondly, I'd like to echo the comments regarding cybersecurity. Now with news about General Alexander leaving NSA, possibly to head up the Cyber Command that we've seen in the press, I think we all believe the Data Privacy Office should have a very key role in that. So anything that we can do to help in that process, we'd be happy to do so. We're curious about the role as well.

And finally, I was very happy to hear about your co-chairing the Privacy Principles Committee for the information sharing environment because I know it's been something that we've been a little concerned about, and it's very difficult given how different agencies classify information, to get to a point where we can all share information in a secure way. And again, we have members of the Committee that have expertise in that area, and we're happy to help as well.

So thank you very much. And thanks to Howard as well for your great leadership.

MS. CALLAHAN: Thanks, Annie. I just had a question about your first question, which is you said is it a social media mechanism to support process as opposed to outreach. I didn't know what "process" meant.

DR. ANTON: So is this to facilitate sharing of information, et cetera, or training, for instance, within government for government employees, or is this something that you view as a mechanism for reaching out to the public and informing the public?

MS. CALLAHAN: It seems to me the latter is the first of these steps, doing public outreach. And as I

explained to Neville, and as we'll explain in our workshop on June 22nd and 23rd, it's pretty complicated. So I think we need to first deal with the outreach portion, and then once we kind of have that locked down and we have the legal and policy and security issues, as I said, addressed, or at least identified and working around, then I think we could go to the training portion.

But I think the outreach right now is the most important, and I think that's the way the public is using it as well. And so that would be -- but again, I'm also not the, as some people used to say, the decider on this.

[Laughter.]

MS. CALLAHAN: It is much more of a -- that's much more of a comprehensive Department-wide approach.

DR. ANTON: Right. I would note that most of the public is online, but we also need to consider that there are members of the public that don't have access to the Internet. And so we need to be thinking about ways to have outreach for those individuals as well.

MS. CALLAHAN: Oh, I absolutely agree, and I want to ask the Committee about that as well. No, I absolutely agree.

With regard to your other two points, again, on the cybersecurity stuff, I think we all keep our fingers crossed in terms of making sure that privacy is part of the conversation.

And on the information sharing environment, that is really important to me, and that really is important to make sure that gets right, and that's why, as you guys discussed, the paper that has been presented by the Subcommittee, I think that's an important thing to consider.

MR. BEALES: Mary Ellen, we've reached the end of our budgeted time, but I would like to, if you have time, if we can continue this and let our schedule slide a little bit I think works fine, but I want to make sure that's -- that we're not holding you hostage here.

MS. CALLAHAN: I'm here all day.

MR. BEALES: All right. Thank you.

Then Joe Alhadeff.

MR. ALHADEFF: Thank you, and I'll join the others with congratulations and welcome and hope that one of the habits from Hogan continues, which is the excellent oatmeal cookies.

[Laughter.]

MR. ALHADEFF: The question I had, which is kind of related to the last question but perhaps a little more general, and that is the concept as we look towards future-oriented technologies, clearly this Committee may be most beneficial in helping provide guidance not after a problem has surfaced but before one has surfaced, so kind of in the anticipatory context.

So as we look at things like cloud computing, virtualization, service-oriented architecture and things of that nature, we were just wondering if those were issues you thought the Committee may have some remit in helping the Department consider, not necessarily at the specifics level but how you see some of those future technologies and some of our work, whether it be in the form of guidance or frameworks or application of existing instruments.

MS. CALLAHAN: No, that’s a great question, Joe. Thank you. And I think, actually, Ramon, your Subcommittee is working on a refined definition of service-oriented architecture, which I think will be very helpful. And I think, again, it kind of is consistent with knowing where the data is, being able to access the data, and being

able to identify controls and responsibilities and so on.

With regard to the anticipatory issues, Joe, I completely agree that what we have to do is kind of project and think how we can tap this phenomenal pool of expertise, and do so ahead of time and not do so after the fact, and that's one of the reasons why I'm trying to help you guys plan and help me plan, so that we can try to look down the road in terms of what issues are coming up. So I completely agree with that approach.

MR. BEALES: Lance Hoffman?

MR. LANCE HOFFMAN: Let me add my welcome and congratulations, Mary Ellen. It's great to have you on board. It's welcome fresh air, your enthusiasm, and your wonderful overview of the scope of the various opportunities and challenges that you have and we all have to face.

I want to take the opportunity to echo what a couple of my colleagues have mentioned. A couple have already mentioned cybersecurity, and I know you know that that's very much on the radar screen, that we can't, of course, do much on it until we see how that's going to come out.

I think it's terrific that the new position of communications director or whatever that position was you mentioned is very important, I think, because it's going to have a very important role, especially if we go out not only to government and training or educating government, and also the public, as you want to, but also we could use it -- I see a big need in academe. We don't have the materials, and to the extent that there's a lot of good stuff that is done here and that could be used maybe with some tweaking, maybe with some targeting, toward the thought leaders and the future generation, we train and a number of people go out every year into government service, and we try to give them as much of this material as we can. And if there were more that were available that could be gotten out easily, it would be very helpful.

The other comment I'd make, echoing Joe, is in terms of future planning. You may want to consider not always having meetings as they are now, where there's a bunch of Subcommittee meetings one day, the next day there's the main Committee meeting and so forth. It may be worthwhile to at some time consider having a mini-workshop. I know the constraints of public meetings and so forth, but

nonetheless, where people could just focus more on the future and less on -- relatively less on having people come in and say, okay, what are you doing in your agency.

MS. CALLAHAN: I will consult with my FACA committee expert and let you know. But, you know, I think we have to see how we go on this, and I think we have to start to project and figure it out.

But in terms of communications and in terms of information, I would love to tap into academe. I think academia is an area where we can learn a lot and, quite frankly, that dialogue has not had as much. So I turn to those who are in the area, part time or full time, for some insight into that.

With regard to communications, I'm really very excited about this position. Toby and Martha had suggested it even before I came on, and I'm thrilled because I really think that it will help hone our message, help hone our information being put out there. And as they know, the privacy website drives me nuts. I think it's terrible.

[Laughter.]

MS. CALLAHAN: And that is one thing that hopefully the new Associate Director is going to work on,

if I'm able to task him or her with anything.

But I think it goes to your point, Lance, where you need to make sure the information is out there. You need to make sure it is available. And I'm also open to suggestions in terms of how to better promote it. You know, I've been taking opportunities to promote, for example, the legal position, as well as the other positions I mentioned today, through other mechanisms, and I encourage you guys to do that as well. I think the more promotion we have on this issue, the more transparency we have on these issues, and the broader pull we have on that I think is useful for everybody, both the Committee and the Department, and for me and the Office. So, thank you.

MR. BEALES: Charles Palmer?

DR. PALMER: Well, by going last, I have to make fewer points. Again, welcome to the team. Glad to have you.

I just wanted to add one comment about the big challenges you have. The harmonization of security and privacy, as others have said, has to take place from the beginning. And as if you don't have enough to do, academia is important for outreach. Increasingly, it's the folks

who aren't quite in academia yet, the K through 12 challenge.

I work with some of these folks, whether it's Cub Scouts or others, and they're out there, and the schools don't really know what to say. And so, like I said, while you have plenty to do, roll this into your outreach if you possibly can; that is, materials for -- we call it K through 16, as the I3P forms last year came to. But this level of outreach is increasingly vital, and I'm not sure where else to go other than the folks who have the biggest responsibility for it in the nation, and that's DHS.

MS. CALLAHAN: That's certainly something we'll consider as we work on the communications plan. To a certain extent, if we have virtual communications, that can help be tailored, taking into consideration Annie's point in terms of those that are offline, intentionally or unintentionally. But perhaps we can think of ways to leverage that communication.

Thanks, Charles.

MR. BEALES: Well, Mary Ellen, thank you very much for your time. It has been interesting and useful to

hear your vision of what comes next. I think we are all pleased to see you on board and look forward to working with you and helping in any way we can. So, thank you again.

Our next speaker today is Paul Hasson, who is the Privacy Officer at US-VISIT. He is responsible for developing a comprehensive privacy program and a data protection framework that ensures that US-VISIT collects and maintains personal information appropriately.

Paul, welcome. We look forward to hearing from you.

US-VISIT PROGRAM UPDATE

MR. HASSON: Thank you, Mr. Chairman. Thank you, Committee. Also, thank you very much for the kind words from Mary Ellen before and Martha for inviting me. I am pleased to be back again. I think it's about eight months ago that I last spoke to the Committee in Las Vegas.

I don't know if you all have the handouts. I know not everybody is facing the screen there, but we're going to proceed. David is going to help me with the screen here.

Since most of you are relatively familiar with the US-VISIT program, I will give a brief, a real brief background and a recent update of where we are, at least since the last eight months, since I spoke to you last.

As many of you know, clearly DHS protects the United States from dangerous people by addressing the risks that people pose to our country. In order to assess risk accurately, they rely on all sorts of tools, all the decision-makers. US-VISIT is one of the key tools, we believe, that helps across the board for immigration, border management operations, for law enforcement, for the Department of Defense, for the intelligence community.

Almost all the different departments and agencies involved in Homeland Security do, in some way or another, use US-VISIT information as a tool, and this slide here gives you an example.

There's a little feedback here, or at least I'm hearing it. Sorry.

So most of the Department does, as well as the other agencies as indicated on the slide there. There are about 30,000 authorized individuals who daily are capable of using US-VISIT as a tool.

Here's a visual depiction of how it stands. Most of the numbers come from those individuals who are seeking entry into the United States via the State Department with visa applications and, of course, CBP at ports of entry.

These are updated numbers, the next two slides, with -- to provide an idea of our general volume we have here. Over 100,000 people a day are involved in the international travel process, whether it's, like I said before, the visa applications or the admission for entry into the United States.

We support USCIS. Citizenship and

Immigration Services works with about 11,000 various cases a day for those individuals seeking benefits, and our BSC, our Biometric Support Center, about 50,000 a week helps identify for state and local law enforcement agencies, identifying the John and Jane Does, the unknowns through our biometric database.

Of note there, there's a relatively small number, the five with U.S. Coast Guard. It sounds relatively small, but since DHS started collecting biometrics at sea, I think it was a little over two years ago, there's been a decrease in those areas of operations, mainly in the Caribbean, by about 75 percent because this was the first time ever that individuals who were caught were actually being prosecuted. So the U.S. Attorney's Office has taken cases criminally.

Also, the Department of Defense and intelligence community do identify terrorists and terror suspects by analyzing biometric information that's normally collected at various sites in theater of operations, like safehouses and training camps. That's why I'm not at liberty to discuss exact numbers, but we are actively working with them.

All together, these efforts are really helping to revolutionize security. Since we began using biometric entry procedures back in 2004, we have seen tremendous difference in our efforts to improve the integrity of our immigration border management system. We stopped more than 4,000 applicants for admission or other criminals who were not otherwise identifiable by their biographics alone. So it's strictly based on the biometrics, in this case fingerprints collected.

We've helped protect travelers from identity theft and virtually made fraudulent documents, the use of fraudulent documents almost eliminated. We've done a very good job with being able to protect that with the electronic passports. And we've dramatically improved information coordination between the various Homeland Security agencies by providing a single source of biometric information for immigration violators, for criminals, for known or suspected terrorists. And building upon these successes, we continue to make enhancements that will improve the services we provide to all these agencies.

Two important initiatives we've been working on and which I know I've discussed before, so I'll only

briefly update you on, was the improvement or the movement from two-print to ten-print, and we have deployed almost completely now, and I know we were on the way there the last time I spoke with you, so covering virtually everybody who we were collecting two prints from at ports of entry. We're just about -- we're just under 100 percent now collecting ten prints. So that's quite a bit of progress we've made.

And by collecting these prints, we've been able to make more quick and accurate decisions for identifying travelers who are both legitimate and not legitimate or where there may be some concerns for entry into the United States.

And also because we're able to more accurately identify individuals using ten prints instead of two prints, it raises our ability to be confident that they are the correct person and it's a more accurate decision, and less people are going to secondary ports of entry as a result.

A little bit about our progress now with biometric exit procedures. Historically, our immigration system has been solely paper based and biographic, of

course, both for recording the entry and exit into the country. Of course, as you know, we've been doing the entry for quite a while. But adding process to biometrically record a traveler's departure, we'll have a faster and more accurate way to determine who has departed and also who has remained here illegally.

Biometric exit capabilities will enable DHS to more effectively enforce our immigration laws and ultimately ensure the integrity of our immigration border management system. In fact, DHS, Congress, and the 9/11 Commission have all identified biometric exit control as a priority to fully secure our nation's borders.

I'll now bring it to privacy. In every biometric transaction, biometric identification transaction, we're cognizant of the need to protect the privacy of those whose information we collect, and we're committed to ensuring that the information we collect is protected from misuse inside or outside the government.

At US-VISIT, we are acutely aware that our success depends on how well we are able to protect the privacy of those who use and interact with our systems. US-VISIT, that's our business, is personal information. So we

certainly value that very much.

US-VISIT has carefully monitored systems and security practices in place to protect the privacy of those whose data we collect and to ensure the integrity of that data. US-VISIT has also a dedicated Privacy Officer -- that's me -- and a relatively robust team considering the size of our program office.

We're responsible for creating a culture within the program where privacy is inherently valued and treated as a fundamental right and obligation and embedded into the enterprise planning and development process. Members of our team are involved from the very earliest stages of planning all the way through implementation and the ongoing operations.

And finally, of course, redress, and that's my main focus here. It's a critical aspect of our privacy policy. DHS and US-VISIT have established a redress process to ensure that all people have the opportunity to have any issues or concerns reviewed in a fair, timely and independent manner. To facilitate such requests, US-VISIT worked closely with DHS to develop the DHS Traveler Redress Inquiry Program, or TRIP from now on, I hope. DHS TRIP

provides travelers with a central online resource for people to submit redress inquiries regarding difficulties they experienced during any point of the U.S. travel screening process. In a moment I'll talk about the other ways besides TRIP, and how we receive requests.

Providing those who interact with our systems a process by which they can correct or inquire about their information is critical to ensuring the integrity of the data we collect. People must have confidence that the information we collect and store is accurate, complete and current.

This -- and I will explain briefly what these mean, but this gives a chart of the types of -- it depicts the various types of requests we get and the volume. Our process enables travelers to resolve these various types of issues by getting a hold of us in the various manners, which I'll explain.

The majority of these requests deal with reviewing whether an indicator alert that flags an individual as a suspect of interest for secondary screening should be deleted or dropped, and that's indicated where it says "demotion review," which is the greatest number; a

traveler being delayed because the system was unable to match his or her fingerprints to the fingerprints on file; and a traveler being sent to secondary inspection because his or her match -- his or her fingerprints and the biographic information on file do not match, and I'll explain that real briefly also.

We also received requests to review a situation in which a traveler was inconvenienced because the fingerprint scan is incorrectly labeled, such as the right forefingers are marked as the left forefingers, and there might have been some error in the transaction.

Finally, we received some requests that do not fit into a broad category in which the traveler seeks to clarify or correct records which we maintain, and certainly we look into those issues as well.

This next slide shows the difference that starting in late 2007 and really last year, with the -- with TRIP being fully operational. We received redress requests through various communications, of course. Primarily it's TRIP, as clearly depicted there. However, we also accept requests through fax, email, standard mail, and even telephone, and we do get them. It just doesn't

seem to be that much compared to TRIP.

Let me give you a few examples of the requests we do receive. The majority of the requests we receive are related to low-quality or mismatched fingerprints or alert watch list demotions, those two areas. For example, with low-quality fingerprint requests, we may continually have difficulty collecting high-quality fingerprints from an individual. So each time they enter the country or apply for a visa, their fingerprints create a record, and they may be sent to secondary inspection to have them verified each time.

To correct this, we will consolidate all the sets of fingerprints records to one record, and the one with the best quality record is the one we will keep as the one attached to that individual. In some cases, traveler's fingerprints may be mismatched to someone else's by biographic information, and that does happen. Before coming to US-VISIT, I did work in the field with CBP for many years, and it does get very hectic. So the number of times it happens is not all that much. However, there are cases where the spouse who shows up to the primary line together with the CBP officer, they swipe both biographic

and -- both documents. So the biographic information is uploaded, and the first document swiped is accidentally mixed with the second individual's biometrics. So that does happen, and we're usually able to determine that pretty quickly, not necessarily on the spot but certainly as they request redress on that issue, and usually they know there's a problem or a potential issue because they were held up to be re-verified.

When a traveler believes they have an indicator or alert that caused them to be sent to secondary unnecessarily and they want it deleted, we review the case to see if the person should be demoted from the watch list or from being on alert. In these cases, we will review the case to ensure that it is an issue that US-VISIT should resolve, because sometimes the individual just may think it's US-VISIT, but it might not be a biometrically-based concern.

If, in fact, the request deals with US-VISIT information, we review all relevant information pertaining to this person to determine whether or not they should continue to be sent for future secondary inspections. In some instances we are able to demote the person from the

watch list or an alert list. So they no longer need to be referred to secondary inspection for that specific situation at least. It doesn't mean that they're cleared for other issues, but at least the one that dealt with US-VISIT and the biometrics.

And as stated there, and that's the only item on that slide, but we take a lot of pride in being timely, and our goal is to complete, end to end, from the time we receive the request until we respond to them with a disposition, within 20 working days. It's not 20 calendar days.

We do have a proven track record for responding quickly. Our average data, as you see there, has been 10 days, which -- and that's average. Some are a couple of days, and some are a little bit longer than 20, but there are various reasons for that. We continue to strive for rapid, fair responses and to continue earning the trust of those who interact with our system, both our stakeholders within the government and, of course, the traveling public.

As the Privacy Officer, I'm responsible for creating a culture of privacy within our organization and throughout DHS where privacy is inherently valued, treated

as a fundamental right and embedded into our development processes. I certainly enjoy the opportunity where I can talk about how US-VISIT is protecting the privacy to our visitors, and again with the theme of transparency, we appreciate getting the word out however we can.

We do not take privacy protections lightly at all. In fact, protecting the privacy of our visitors has been one of our core guiding principles since our program's inception in 2003.

We look forward to continuing to work with the Committee, as I hope to be back again to speak with you all, and that's all of my prepared comments, and I look forward to answering any questions or responding to any comments you all may have.

MR. BEALES: All right, Paul. Thank you very much for being with us.

We'll start with Ramon Barquin.

DR. BARQUIN: Thank you, Paul. Good presentation. I've got three quick questions.

First of all, from the point of view of the mechanics, how long does it take for the average entrant into the U.S., I mean just the mechanics of it? You've got

now the ten-print, the biograph, et cetera, et cetera.

The second question is do you -- I mean, I gather right now your database is exclusively what you have started to collect history from day one of US-VISIT, or have you enriched it with other biometric information from other agencies?

And the third is architecturally, how does this sharing happen? I mean, you had a whole bunch of different agencies that interact and query and use your -- architecturally, how does that happen?

MR. HASSON: Thank you. I'll be happy to answer all three questions as best as I can.

First, regarding the primary response times at ports of entry, or not response but the processing time, number one, I'm no longer CBP. I'm not sure that I want to speak freely about, you know, what their -- I don't know their exact times. However, what I do know is that we -- when we rolled out both the electronic passports and the ten-prints, which I had the opportunity to participate in both rollouts out in the field, the technology was actually improved, the end-to-end technology. So where part of the process might have seemed a little bit longer than before,

it actually -- the technology side has made up for at least part of that.

Also, with moving from the two-prints to the ten-prints, on all subsequent re-entries into the United States, or if we've already had the ten-prints on file through the visa application process, then we just do a verify, and the verify is only composed of a single slap or a single placement. So it's only one motion instead of the old two, which was required with the two-print. So I've not heard much in the way of further delays. And again, CBP field operations can probably speak better to that, and I can look back to that if the Committee would like that.

Regarding the database, yes, it's composed of not just the -- all the various agencies where we have a working agreement, as listed on whatever it was, I think it was the third slide, it's both input and output. So these agencies are contributors just the same as recipients.

Yes, some of the information is historical, certainly, and some of it is new, or a lot of it is new I should say, as we are enrolling new people, and those are also clearly identified in our Privacy Impact Assessments, how we operate.

DR. BARQUIN: My question is really related -- let's say, for example, that you have someone, that you have a totally clean passport biographic document, but it is someone that's a bad guy, and you may not have them in your history as a bad guy, but someone else might in another database. Do you enrich that as part of the process?

MR. HASSON: For IDENT, which is our main database for US-VISIT, along with ADIS, which is the Arrival and Departure Information System, IDENT is biometrically based. So if an individual is, to quote you, a bad guy and has been arrested and fingerprinted, then we would indeed have the opportunity to have their fingerprints on file, even under an alias, whether any of the other biographic information is different, the name, the date of birth, passport number, even country. So hopefully that made it a little more clear.

And then regarding the third question, which was how other agencies' queries are able to obtain our information, unfortunately I'm not a technology guy. However, from a policy perspective, we engage with them from the onset with various types of information sharing

agreements, whether it's service-level agreements, memorandum of understanding, those types of documents. And what we're able to do is set up the standards for the security and the privacy issues, which include access, retention, redistribution, all the important elements. But as far as the technology of the lines, I'm not prepared to answer that.

MR. BEALES: David Hoffman.

MR. DAVID HOFFMAN: Thank you, Howard. And, Paul, thank you very much for coming here today. The Committee has had the opportunity to take a look at US-VISIT a couple of times in the past, and having you be able to come back and spend some time with us is very helpful.

The first question I wanted to ask -- and I also have three quick questions, I swear to my fellow Committee members -- what is the current setting for the data retention for the biometric information that's collected in US-VISIT? And then I want to follow up after.

MR. HASSON: Okay. The -- in our SORN, we have it stated as 75 years for data retention.

MR. DAVID HOFFMAN: And that's what's also not just in the SORN but that's what's in the system?

MR. HASSON: And that's for IDENT, right.

MR. DAVID HOFFMAN: So I guess my -- I'll make a comment on that. I think generally most folks would think that 75 years is on the outward bounds of what many might consider to be reasonable in most situations.

So that leads into my second question, which is beyond redress, and I appreciate very much the redress information that you shared with us, what efforts are there to reach out to the individuals who potentially might be impacted or representatives of those individuals to understand what -- to educate them on US-VISIT and to understand what concerns they might have? And I'm thinking particularly it might be foreign governments who might be representing people who would be coming here as guests to our country to spend money and help our economy with tourism.

MR. HASSON: Fortunately at US-VISIT, not just our privacy program has been well developed from the onset. So has our public liaison and communications office. They have a staff who seems to me at least, from sitting in the office, constantly on the road. They do get the word out. We make sure that the privacy issues are relayed, not just

our formal documentation but our practices, and we want to make sure that everybody understands how US-VISIT is able to handle any kind of inquiry, but especially redress.

Now, beyond that, part of our spike in overall redress requests I believe is attributed to the development of TRIP, and I think that TRIP has been able to really get the word out through the various users. I think CBP, certainly from US-VISIT's perspective, I think CBP has really promoted the use of TRIP. I believe that it's -- the fact that it's easy to use, that it's online, and that it's kind of a one-stop shop has helped publicize the redress process.

MR. DAVID HOFFMAN: Can I follow up, then?

MR. HASSON: Yes.

MR. DAVID HOFFMAN: And just understand, since you're getting that kind of feedback, what feedback are you getting on the 75-year retention policy? Because I can understand it theoretically. A two year old who might visit the country might then, when they're 76 years old, decide to take on another alias. It's just that as we balance the potential risks to privacy versus that potential risk, that seems rather remote.

MR. HASSON: Right, and I appreciate that. To clarify also, and perhaps it should have been in the overview, we only collect fingerprints on those between 14 and 79, not -- but still, the point --

MR. DAVID HOFFMAN: So the 14-year-old you then would be worried about when they're 88 years old.

MR. HASSON: Right. No, I just wanted to clarify that. But nevertheless, that is -- I have not received comments from individuals. However, the agencies with whom we work have shown concern with that. And based on their PIAs and their standards that they've set, we will adhere to their requests.

For example, if an agency says that they're going to collect prints for -- and this is hypothetical or theoretical -- for employment purposes to work in their agency or to be credentialed, and they're only allowed to keep the prints for one year after their employment, then we will adhere to that. And I know this isn't about entry, but regarding at least in other uses. We do, like I stated, much more than the entry and exit process. But based on their request, we will take them out of -- we will delete it from our system.

MR. DAVID HOFFMAN: That's helpful, and I think maybe we can just take it as a follow-up item to take it up with the Privacy Office to have more of an understanding of why 75 years is a necessary retention period for that data.

The last question I have real quickly is you note in your slides that there's going to be two biometric collection scenarios in the summer of 2009 for the exit process for airports and seaports. I remember seeing on some of the tours that we've done in the past the great challenges in the airports with doing exit, given space requirements and being able to get -- I'm wondering if you can share more information on where those tests are going to be done and how you believe they're getting around those challenges.

MR. HASSON: Yes, I can briefly. It will be happening very shortly. In fact, notice will be coming out I believe in the next week or so, public notice on that.

Unfortunately, a couple of the -- there's been a couple of logistical changes as far as location, so I'm not sure I want to state at this point. However, what I will say is that at two -- it will be limited to two airports. They will be run by -- these are mainly pilots

of the technology more than the process, because we do understand the challenges, as you stated, with the space at various airports.

So two of the DHS entities, TSA will work at one airport at a screening area, and Customs Border Protection at another airport by the jet ways. And it will be for a limited period of time. I believe it's 30 days, really testing the technology and the high-level capabilities. As far as a comprehensive plan, that has not been developed yet.

MR. DAVID HOFFMAN: Thank you.

MR. BEALES: Annie Anton?

DR. ANTON: Thank you for coming to meet with us again, Paul. We appreciate it.

I appreciate your goal to respond to redress requests within 20 work days, and I'm curious about, firstly, what percentage of TRIP requests actually take longer than 20 days; and secondly, what are the characteristics of those particular requests that do take longer than 20 days, and what kind of complexity are you dealing with there?

MR. HASSON: Thank you. That's a great

question. First to clarify with the 20 days, that's the time we receive it at US-VISIT. So we'll go to TRIP first, and then they will send it to us, to our team, and that's when our clock will start.

And the types of cases that would take longer than 20 days are most frequently the ones where it's the quality of the fingerprints issue, and we will send a letter back to the requester that explains to them the concerns about the quality of their prints and we are not able to get a clear verification upon their entry.

We kindly request that they resubmit a fingerprint card, and in most cases they do. However, a lot of the cases they are international, so there is that time. The clock is still running during that time period for them to receive the letter, send it back to us. Almost immediately once we get the card, we're able to take it down to the biometric support center and match that up, and that's really the type of case that takes over 20 days, and that could be 30 or 40.

DR. ANTON: Thank you.

MR. BEALES: Joanne McNabb.

MS. MCNABB: Thank you, and thank you for

rescuing my little thing here, my tent.

I have a couple of questions, too. You said that you have -- I think I just didn't hear it all -- stopped 4,000 or over 4,000 bad guys who were not otherwise identifiable without the biometrics. What time period is that?

MR. HASSON: Since January of 2005 when we went live.

MS. MCNABB: Okay. And then what are the conditions under which local law enforcement can access your biometrics? Is it a warrant?

MR. HASSON: October of 2008 we published a PIA on our interoperability with the FBI CJIS APIS system. Through that interoperability, state and local law enforcement agencies who are signed up to participate in this program actually do it through CJIS, through the FBI, and then it gets sent to us, so as they have somebody who is in custody. So these are not traffic stops or randomly going up to people on the street. These are people who are already in custody who are being booked and fingerprinted.

MS. MCNABB: And I obviously don't have a lot of technical knowledge here. It will become obvious as

soon as I continue with this question. My understanding -- so we're not talking about biometrics. You're talking about a template that is being matched in an automated fashion. You're not talking about looking at pictures of fingerprints, right?

MR. HASSON: Right. This is automated.

MS. MCNABB: Yes. So how does somebody outside of US-VISIT use that template to compare it to whatever they've got, which presumably wasn't collected in the same system, producing the same sort of template?

MR. HASSON: I think we're on even par with our technology expertise. But what I can say operationally and what I am familiar with is that the standards are already established before we go into agreement to operate with them. So we know they're able to read each other's prints, if that is your question, Joanne.

MS. MCNABB: Yeah. I probably need to get some -- I really want to know technically how -- whether -- to what extent it's possible to compare biometric templates of prints from two different systems. That's -- you don't know, and I don't know also, so there we are.

MR. HASSON: They're able to communicate.

MS. MCNABB: Somehow. So they may be comparing images rather than --

MR. HASSON: It's images that they're comparing, absolutely.

MS. MCNABB: Okay. So they're comparing images, not the templates.

MR. HASSON: I believe so, and there are certain points, and I have a feeling part of the -- there might be Committee members who might understand the technology a little bit better, but I do know that our experts in the biometric support center, from hearing them talk about the various points to match up and what-not.

MS. MCNABB: Yeah. Thank you.

MR. BEALES: Tom Boyd?

MR. BOYD: Thank you, Howard. And thank you, Paul, very much for joining us this morning. My question really relates to your redress policy. To what extent is there follow-up with those visitors who have been inconvenienced by virtue of false-positives or options that proved to be false? Once you've had your redress process and you've determined the basis for it, what follow-up do you have?

MR. HASSON: We have 100 percent follow-up. Everybody receives a response, if that's your question. We respond to them with a disposition, sometimes not in great detail because of certain sensitivities. However, we -- because I write and send off every letter, or my team helps me with preparing it. I sign every letter. But everybody receives a response.

MR. BOYD: Okay. I guess my principal concern was I understand that there's the official response and disposition of the inquiry, but I was concerned about the extent to which people are inconvenienced, what kind of thoughts they may have. They may have some suggestions or thoughts about how you might improve your procedures. I didn't know if there was any kind of follow-up like that.

MR. HASSON: I'm trying to think of cases where that is really -- I've not seen it so much. Once in a while they will provide narrative beyond just the facts of what they experienced, and based on my experience and working at ports of entry for many years, how to handle those situations again in the same written format as carefully as possible so they can realize that we understand the situation.

There are cases where -- I mean, we're only able to respond really to the biometric aspect of the entry process. There are cases where there might be multiple issues or issues that weren't even US-VISIT related, but they still share their opinions and concerns with us. In those cases, if we receive it, we will forward it to TRIP so it's forwarded appropriately to who we believe is the appropriate agency. But we try to handle as best as possible the cases that apply to us.

MR. BOYD: Okay. Thank you.

MR. BEALES: John Sabo?

MR. SABO: Thanks, Howard. Thanks, Paul.

Two questions. One is, essentially, are you -- so the first question is sort of a technical match question. I can't recall this from the prior material, but are you matching the biometric element against a data record? In other words, you've got an identifier, a passport or some other identification document, and associated with that is a biometric identifier. Is that the match, or is that plus a search against other biometric data? Do you --

MR. HASSON: If the individual has already

enrolled in our system --

MR. SABO: If they're enrolled already, right.

MR. HASSON: Right. If somebody is enrolled in our system, we do apply an enumerator, an identifier where it's associated with a single individual by the biometric. But as far as, again, the technology part of it, I can certainly reach out and --

MR. SABO: No, I'm just curious. We may have that in prior material.

MR. HASSON: Yeah.

MR. SABO: I was trying to determine if, for example, if they're enrolled, it's a fairly direct match against a biometric data. If they're not enrolled and they've got to enroll, that's a separate issue.

MR. HASSON: Oh, right. What happens is we, on a normal case, we will run the biographic information. If we believe we know this individual biographically, then we're able to do a quicker match. In other words, we can do a verification, and the system will inform the operator that we're just going to do a verification of a single print. If our system does not know the person by the biographic information provided at that point in time, then

we will require a ten-print. Speaking operationally here, exactly how it works technologically I'm not sure, but it does a search of the entire database upon the application of the ten-prints.

MR. SABO: Okay. And the second question is a little more general, and you may not be able to answer it, but you may. The U.S. is basically creating a whole new methodology related to entry into the country for non-citizens, and other countries will be adopting similar strategies. So the question in reverse for U.S. citizens, have you been approached by other countries which are considering or about to implement similar biometric identification about your procedures and U.S. policies and procedures? Are you aware of that, and have you been involved, and what do you see as the implications for data privacy for U.S. citizens? Which would ultimately lead to our requiring redress and our encountering issues as travelers to other countries. Can you talk about what you've been doing in that space?

MR. HASSON: I can say or what I do know for certain is that we do have a team dedicated -- again, we have a lot of teams at US-VISIT, apparently. But we have a

team dedicated to working with our international partners. We do know that there is heightened interest in, as you stated, using biometrics upon entry.

From a privacy point of view, I have not worked in any of those planning activities. However, as Mary Ellen stated, when they've had foreign visitors come to the DHS Privacy Office, they've been kind enough to invite me to participate in discussions. Those specific issues haven't come up. They're at a much higher level than working on biometric entry. But I do feel that we would be engaged at some point.

MR. SABO: I mean, I think that goes back a bit to David's point. We -- some of the policies that we set become a benchmark for other countries, and there may be countries where they may or may not have equivalent security and privacy protections that we expect and we have in the U.S., and I think that raises questions that we're setting a baseline. For example, a 75-year retention rate might be viewed as, well, that's a U.S. standard, and now we as travelers to other countries will have similar issues. So it's something that maybe the Committee needs to -- there may be opportunities for the Committee to look

at those issues for reciprocity and equivalency and policy issues.

MR. HASSON: And we certainly, we look forward to working either with our partners or with the Committee or DHS Privacy Office on that. Thank you.

MR. BEALES: Neville Pattinson?

MR. PATTINSON: Thank you, Paul, for your very informative presentation. I guess I'm the techie in the room. I have a lot of knowledge on the e-passport program from my professional career, but I will recuse myself from specific issues about that and ask you about your program.

Regarding the good words you said about reducing document fraud, I think that's a good sign of an electronic passport introduction. What kind of percentage do you think you're seeing as far as foreigners coming to the country with electronic passports now? That's kind of the first question, because it's still in issuance around the world.

But then as far as your own procedures, obviously you're reading biographical information off various pieces of the passport. Are we storing that information in US-VISIT? Is that sucked off and stored?

Equally, the photograph electronically, are we capturing that from a camera, or are we taking it from the electronic passport? Are we storing that?

And then we have European countries and other countries that will now add fingerprints into their electronic passports. Do you see that being accessible to US-VISIT on arrival?

MR. HASSON: No. Okay. Regarding the percentage of passengers using the e-passports, I do not have those numbers right now. Certainly, as we know, all the visa waiver countries are required to have them. I'm not sure what percentage of them actually are arrivals into the United States and probably could get those numbers from CBP yet again.

Regarding the information that's on the e-passports, that information actually -- the information that we do store with US-VISIT and IDENT is the information that's collected strictly for the purpose of IDENT, which is upon the arrival or at the consulate office. Information that is within the passport itself is open, so to speak. I don't know the proper technical term, but within the chip it's open and it's presentable to the

operator, to the officer at primary. And what they're able to do is confirm that the biographic data, including the photograph that's embedded technically or technologically into the document, is the same as the picture on the document itself and the individual standing in front of them.

MR. BEALES: Charles Palmer.

DR. PALMER: Again, thank you for coming.

More geek questions, I'm afraid. On Slide 12, you talked about the types of redress requests in 2008. I just have these two questions.

The first one on that slide is do you have any feel or can you share any of the results of those, however many that adds up to? Were they all made happy and went away, or were some told sorry, or how did that work out?

MR. HASSON: We -- I don't have the numbers handy, but what I can say is from actual responses that are provided to the individuals, there are many of them, especially with the demotion review, where individuals who come in -- and the number spiked -- I don't know if it shows it here. Actually, in 2008 it shows one of the spikes was because of TRIP. The other is, that's when we

were pretty much fully operational with ten-print.

Once we started collecting ten-prints, that information we were receiving, that was also being run with the Criminal Justice Information System, with FBI. We would get accurate criminal information, and it would be then sent back to IDENT. However -- so on a subsequent re-entry, or a subsequent entry by the individual or by the traveler, they would be referred based on that alert.

It would be determined usually pretty quickly from reviewing what the origin of the alert was it was the right individual, the person was indeed arrested or convicted, whatever the case was. However, it was not a crime that made the individual inadmissible. On those cases, when we're made aware of it either by CBP or the individual, we will go in and demote it. We will take it off the alert from US-VISIT. Obviously, we cannot take it off of the FBI system because it's still a criminal act. But that's pretty common.

With the mismatches, frequently when we see that, it's a very easy fix when it's like the example I gave with the spouses swapped prints from the biographic. Because we also take a photograph, it can be instantly told

that somebody who looks like me should not be named Susie, for example, and you can see it from the picture, and then they would be able to see the timing and everything else, and then they just rearrange the prints.

DR. PALMER: Okay. Second question, then.

MR. HASSON: Yes.

DR. PALMER: You mentioned you do leverage data from other sources, like hiring and this person has joined our agency sort of thing. Is that data tagged in some way to show that it came from that agency so that if they do inform you at some point later, saying X is no longer working for us --

MR. HASSON: Yes.

DR. PALMER: -- or that agency has a different retention policy, is this information tracked that way or tagged?

MR. HASSON: The source of the data I believe is. However, how it's done, I'm not sure. But we are able to identify them when the request for demotion or deletion, usually in those types of cases, comes up, and we're able to find it quickly. I'm not sure if it's automated or if you press a button and say everybody from this timeframe

from that origin, or exactly how it works. But I think the take-away is that we are able to delete them.

DR. PALMER: And just to pick on you --

MR. HASSON: Okay.

DR. PALMER: -- the deletion rate, I mean, do you actually see maybe thousands of records added a day and a few hundred were deleted each day?

MR. HASSON: I know the number -- our overall gallery is not decreasing. If anything, it's increasing. I believe we're about 97 million records, biometric records. I do know from asking, because this question has come up before, that every day there are deletions, but it's certainly not the volume that we're increasing. So I would say yes, we are deleting every day for various reasons. They might even be the FBI where a criminal record is expunged and they notify us, so we take it out of our system if it's information that they provided to us, or a good example is the other agencies where their data retention period expired, so we have to delete it as well. So every day, yes.

DR. PALMER: But they're telling you to delete it, not that it's tagged with the data saying this is 60-

day data.

MR. HASSON: That is correct because we have no way to know if somebody has left their employment, for example.

DR. PALMER: Sure. Okay, thank you.

MR. BEALES: Dan Caprio.

MR. CAPRIO: Thank you, Howard. And thanks for your participation today, Paul. Just a quick question. Thank you for the explanation of the pilot projects this summer.

I'm just wondering, on the slide you mentioned the expectation to finalize procedures by next year, is it the expectation that all land and sea borders will have the biometric procedures? I mean, you talked about the two pilots. Are we talking about nationwide by the end of 2010?

MR. HASSON: No. I believe the 2010 timeframe was to expand to the rest of the air and sea, or at least the air. The land, there seems to be a lot of work and a lot of logistical planning that would need to take place. Based on the various recommendations, or even mandates to have it done, it will certainly have to be comprehensive

exit, biometric exit ultimately. I do not know the timeframe for the land as well. I do know that we've been doing a lot of the preliminary planning work already.

MS. LANDESBERG: Renard?

MR. FRANCOIS: Thank you very much for your presentation, and congratulations to speaker pro tem, chairman pro tem Annie over there, for your recent ascension.

[Laughter.]

MR. FRANCOIS: I have just two questions for you, and the first relates to you made a comment about information sharing agreements that you have in place with the agencies with which you share information. And it's -- my question centers on whether there are any audit procedures or protocols that you all have in place to ensure that the data that is being shared is being used in a way that is consistent with what's in the agreement.

And the second question -- and to the extent that there are, I'd love to hear a little bit more about it, and I might have a follow-up question or two.

And then the second question, at the risk of beating a dead horse, relates to the 75-year record

retention rate. And the reason that's of interest to me is we've heard in a number of other venues about record retention requirements that have different time periods. On one trip we heard about a 90-year time period. And there may very well be good reasons for treating certain elements, certain data pieces and retaining them for different periods of time, but it doesn't seem to be a time period that's mandated by law. It doesn't seem to be a time period that has an articulable rationale, and not just yours specifically but those kind of differences, and I'm just trying to get a sense of how these programs are coming up with these kind of disparate time periods.

MR. HASSON: Okay. To answer the first question, regarding the audit, internal DHS is not so much for -- we have access. We see what's going on, and we work internally. That's not a concern. Where we have the audit concerns and where we've written them into place in the MOUs are with our external stakeholders.

This has all been -- these information sharing agreements are all relatively new. I mean, even though the program is relatively new, last five years, just over five years of going live, January 2004, really in the past year

or so. Although we have established a policy of having the capability to audit, the IT security team and the IT operations and maintenance, O&M, work out the details. I'm not sure of what the exact details are, so I don't know if I'm prepared to answer that at this point. It's just because I, quite frankly, just don't know it. But I do know that we make sure that that's in place when we set up these agreements.

Regarding the 75-year retention issue, it's up to 75 years, for one thing. But I cannot speak on behalf of the other agencies, whether some are 90 years or some are a lot less years, and obviously this has sprouted as an important issue, and we look forward to working with the Committee, or a Subcommittee, or the Privacy Office on dealing with that. At this point, it was established before I came on board, and I can't really speak to the history of it.

MS. CALLAHAN: If I may just try to help clarify, Renard. And excuse me, Paul, or should I call you Susie?

[Laughter.]

MS. CALLAHAN: The information sharing

agreements for US-VISIT and across the Department should all have in place applications of the Fair Information Practice Principles that the Department has endorsed. In terms of the retention and in terms of the use and the restrictions and so on, that should be memorialized in these information sharing agreements. We're also going to get more enlightenment from the Subcommittee paper that was done here within the Committee.

With regard to the retention, as you know, Renard, those are all driven by the records administration focus, and it doesn't necessarily mean that our colleagues can keep it for 75 years. What it means is we as the Department can keep it for 75 years consistent with whatever the System of Records Notices and whatever the records retention on that information is. So that is kind of a separate regulatory structure, separate and apart from what the information sharing situation is.

Did that help clarify it a little bit?

MR. FRANCOIS: It did, and my concern is just I've heard different numbers. There may be very good reasons for keeping things for longer periods and keeping things differently, but it doesn't -- I haven't heard a

rationale for here's why we keep this up to this long.

MS. CALLAHAN: You see, you're looking at this rationally. That's the problem. No, I will -- here's, I think, the conundrum that you're facing and that we're facing, is that each of these systems and each of these processes grew up kind of siloed, so to speak. You know, Custom's information was collected by Customs and was kept in a paper form, and fingerprint information was collected by the FBI and kept in a paper form, and all of this was kind of kept siloed, so they each -- they grew up separate. They grew up separately where they had their own System of Record Notices, they had their own records retention standards and issues and so on. So they each did it separately.

Now as we get to the information sharing agreement, I think a secondary or tertiary issue is trying to resolve these retention issues. I candidly will say I don't think it's a primary issue because first we have to make sure the information sharing environment is operating effectively and appropriately. But I hear you, but that may be a little longer-term goal.

Sorry. Didn't mean to interject, Paul.

MR. BEALES: Lance Hoffman.

MR. LANCE HOFFMAN: Thank you for coming in and talking to us again. I think I heard you say something earlier about you have a 20-day goal for responding to people, but you made it clear that was the US-VISIT response and not, for example, the TRIP response. Am I missing something?

MR. HASSON: Correct, our goal. I can only speak on behalf of our office. I'm sure that TRIP has a standard that they try to match. Certainly the volume they receive since they are, as I stated, the one-stop shop for all traveler-related redress issues. So, yes, for us specifically it's 20 days.

MR. LANCE HOFFMAN: Well, that gets to my question, which is how much integration is there? And this doesn't apply only to US-VISIT but also to the Department in general. If TRIP is the one-stop shop, the user experience, the user typically, the citizen, whoever the foreign national, whoever goes through TRIP, it eventually in some cases goes to you. You come back. Do you give the information back to TRIP, or do you go directly to the questioner?

MR. HASSON: We actually send the response back to the requester.

MR. LANCE HOFFMAN: So TRIP never closes the loop.

MR. HASSON: And we close it through TRIP, because TRIP is an automated system.

MR. LANCE HOFFMAN: So you close it through TRIP, but the listener -- what's the perception, is my question, of the foreign national or whoever is making this query? I'm worried about things getting lost in the cracks and that sort of thing. This may not be -- this is really not a US-VISIT question, but I want to point out it sounds to me like there's a potential here for problems.

MR. HASSON: I hear your question, and we actually respond from TRIP and close it through TRIP on standard-type cases where we were the ones to -- if they went through TRIP, we will close it out as if it were through TRIP, and correspond with TRIP simultaneously.

MR. LANCE HOFFMAN: Okay. All right. Okay. Thank you.

MR. BEALES: Joe Alhadeff.

MR. ALHADEFF: Thank you. I kind of wanted to

revisit the complaint concept, and I've got no doubt that the answering of the complaint happens as stated. My concern is that I travel a lot and I've interacted with a lot of people from a number of different countries, and I get the impression that a lot of people don't complain because they feel somewhat intimidated at the point at which the complaint would most normally be made.

And so it might be useful to do a survey to see the impression of the actual process rather than whether or not a complaint is elicited, because I think there might be a higher level of incidence of people feeling that the process did not treat them fairly or in a courteous manner or in a professional manner than is perhaps coming to you in the form of formal complaints.

So has there been any concept of actually doing some kind of survey or using some kind of opinion tracking to find out if the impression of the welcome mat is a little more threadbare than we'd like it to be?

MR. HASSON: I can certainly appreciate that question, especially with my time working at a port of entry and the various cultural differences of individuals arriving or applying for admission into the United States

and how they might feel about potentially complaining or raising any concerns.

I think that -- and I'm not 100 percent sure how the TRIP word gets out at the port of entry. I had left the field already when TRIP started. I left the field in 2005, and 2007 is when TRIP started. We were concerned about -- even when I was still at CBP, we were concerned about public perception and professionalism and making sure that people were communicated with appropriately. From looking at our numbers of requests we get through TRIP, I believe that the word is getting out about the ease of use of TRIP.

Again, I can't get in the mindset really of the intimidation factor or fear factor of individuals. I do know that our, as I said before, our public liaison and communications team tries to get the word out there and let them know about easy access to their information, please let us know. We have, like I stated, I believe it's five different methods to reach us, and we do our best from our end. We are the side that the public never sees, though. We're in the background. We're just a tool. We're not the operator.

MR. BEALES: Paul, I want to thank you very much for being with us today. This has been very helpful and informative, and we appreciate your time, and I'm sure we'll hear from you again.

At this point we will take a break for about 15 minutes. We should resume at 11:15.

[Recess.]

MR. BEALES: All right. Thank you. Our next panel will give us an update on the E-Verify program and hopefully something about what's become of our recommendations on that particular program.

We have three speakers, all from the Verification Division of U.S. Citizenship and Immigration Services, which is where E-Verify lives.

Our first speaker will be Katherine Lotspeich, who is the Deputy Chief of the Verification Division. The division oversees the E-Verify program, and also the Systematic Alien Verification for Entitlements program, otherwise known as the SAVE program.

Also with us is Michael Mayhew, who is the Acting Chief of the Operations Branch in the Verification Division. He manages special projects and initiatives for

the E-Verify and SAVE programs.

And our third speaker will be Elizabeth Dennison, who is a Management and Program Analyst in the Division. She works on the Division's special operations team and serves as the lead on the E-Verify registration reengineering effort, and is a 2007 Presidential Management Fellow.

So welcome to all three of you. We look forward to hearing about where the program stands today, and we'll begin with Ms. Lotspeich.

E-VERIFY PROGRAM UPDATE

MS. LOTSPEICH: Thank you very much, and I want to thank everyone from the panel and members of the public that are attending here today. It's good to see that a lot of the types of organizations that we hold a dialogue with fairly regularly also came today to this particular panel to hear about our updates and initiatives that are in line with your recommendations.

The E-Verify program is continuing to grow. We are gaining about 1,000 new employers each week joining the program. We're up to about 125,000 employers right now that represent about 400,000 work locations or business locations in the United States.

While we're experiencing this growth in terms of program usage and new employers, we're also continuing looking at ways to improve the program from a usability perspective, from a policy perspective, from a technology perspective, and then also as well from a privacy perspective. And we welcome very much the recommendations from DPIAC (inaudible).

Now, the first time we've had the opportunity to meet with you all, I think we've had about two meetings

up until this point, and when we saw your recommendations about four or five months ago, I think, it was a really good sort of -- it's a litmus test for us because a lot of the things that you had recommended are issues that we recognize as well, things that we are already grappling with, figuring out what are the best solutions for us right now.

I also wanted to mention that we are the only division in USCIS that has its own Privacy Office. We started a Privacy Office about maybe 14 months ago just about. We brought over some of the Privacy Office experts from US-VISIT, and we have a small staff there of about eight people that just work on privacy issues for the Division. We have a representative from our Privacy branch in each of our branches throughout the division.

So we're looking at privacy issues across the board, not only on the technology side of E-Verify but things such as our phone center, how we manage outreach events, how we store information and relay information internally, how we look at special cases that need to be resolved and quality assurance programs.

So we're very much in tune with your world,

your perspective, and we look forward to talking in more detail today about your recommendations. And with that, I'm just going to turn it over to Michael Mayhew and Liz, who will walk you through specifically the recommendations and initiatives that we're working on right now.

MR. MAYHEW: Thank you very much, and thank you to the Committee for letting us speak today and for the recommendations that you submitted. We intend to walk you through the PowerPoint and hopefully get a lot of questions in regards to the work we are doing to address the recommendations you've given us, and hopefully any other questions about the E-Verify program.

To walk through the slides, the purpose is to basically review and align the future state registration process with the DPIAC recommendations. We thought to walk you first through what is E-Verify, very briefly, summarize also your recommendations, and then go step-by-step and what our responses are both from the program and from the policy end to address those recommendations and what we're looking to do to improve our registration process specifically.

Background. What is E-Verify? As most of you

know but maybe some don't, it's a Federal Internet-based program run by the Department of Homeland Security in partnership with SSA. It was developed as part of a growing concern in the U.S. around illegal immigration and unauthorized employment. It's a complement to the Form I9. The Form I9 is required for all employees in the country, and what the E-Verify program does basically is run I9 information against DHS and SSA databases.

It was previously named the Basic Pilot, and it lets employers verify work eligibility for all new employees.

Summary, very quickly, of your recommendations. First and foremost, assess the security and privacy risks using NIST and OMB guidance to evaluate, select, and implement controls appropriate to that risk.

Second, explore options for establishing an employer identification and authentication system, and we'll particularly concentrate on that one.

Third, consider the use of commercial information sources to verify the identity of employers registering to access the system.

Identify and authenticate all individual users

of E-Verify.

Develop alternative registration and authentication methods that reflect existing levels of trust associated with the types of employers or third-party service providers.

And lastly, implement audits and take steps to penalize and publicize fraudulent uses of the E-Verify system.

Recommendation one, assess security and privacy risks. We have had a ton of formal system assessments, and I lay a lot of them out there, and I won't go into them specifically. But we have all current security assessments for the system being done and continuously being done in the future. So we are in line with all security and privacy risk assessments that we need to be.

A little bit about what our registration reengineering initiative was about and how we came to the conclusions that we came to in addressing your recommendations. We conducted 30-plus interviews with internal and external stakeholders to identify risks and requirements for the future state business process. One of our key findings from that, and one of the things that

continuously came up in these interviews was the importance of validating the organization that signs up. We need to know our customer better, our customer being employers, and validating customer information in the registration process is very important.

Beyond company validation, three main things came up: improving the process so that it's more usable; enhancing security; and improving the quality of the information that we have in our system. And designing an inclusive design environment, ensuring involvement of division stakeholders across multiple disciplines -- IT, privacy, program -- so that we have all interactions with our customers kept in one central place that is secure and that is in line with all privacy guidelines is very important.

Recommendation two and three, which touches on what I just brought up, which is validating the organization. One of the recommendations was using the EIN to authenticate a company's identity. That was brought up in the recommendations submitted by the Committee, and we have run into some problems with that based on the IRS Code 6103, which prohibits use of tax data for outside purposes. We

looked at a few potential work-arounds, but they were too burdensome. We talked to the IRS. They did not seem as willing to go that route, but we have continuous discussions with them.

In the new registration process that we're designing, and there's a graphic at the bottom, company information we are looking at vetting through a third-party database to flag companies for communication monitoring and to initiate compliance assistance early in the E-Verify customer relationship. It's important to point out what we are proposing is not denying registration to anybody up front who registers, but we are looking to vet the information supplied by the employer against a third-party database as a way to target our monitoring compliance work to those companies who are not being checked out.

We are looking at a few third-party databases that have that ability and are working through a couple of proofs of concepts to see what a matching algorithm would look like.

Recommendation four was identify and authenticate all individual users. One of the things in our future state registration process that we're looking at is role-

based registration to ensure that individuals who register have certain roles and profiles and have use rights associated with those so that not everybody is granted the same amount of access to the system and the same amount of access to information in the system.

We are also looking at adding email validation so that if I go and try and register as a new user, I will be sent an email and will have to have that email authenticated as an initial step. Longer term, we're looking again to third-party databases as a way of authenticating that individual user so that we have an idea of who their identity is.

But as laid out on the side, we kind of came up with five particular roles: a registrant, which is somebody who has been assigned to enroll the company; a program administrator, which is kind of the day-to-day administrator of the E-Verify program of a particular employer; the executive POC, the executive point of contact, if there was a compliance matter that needed to be addressed, an executive person who we could contact first; an MOU signatory, who we're imagining would be somebody in the legal office; and then a user who would report to the

program administrator. And different use rights associated with all those roles was a way of further securing the system and dealing with privacy concerns where certain users were having too much access. So to assign roles we thought would be a better way to handle that.

Longer term, as I mentioned, we'd like to identify and authenticate all individual users, and we're working closely with our Privacy Office, both in our division at USCIS and at DHS, on different ways that we can do that and leverage third-party databases, because we do share the concern that access to the E-Verify system for any user is a privilege and something we would like to gain more identity assurance of the users of our system.

At this point, turning it over to Liz Dennison to walk you through the rest of the presentation.

MS. DENNISON: The next recommendation builds off recommendation four, really, and it's to develop alternative registration and authentication methods that reflect existing levels of trust. So as Mike just went through, as part of the registration process, we're looking at defining user roles through registration that will have different levels of ability to go in and use the system,

and we recently put together a team that will look at creating profiles within the actual users of the system, past the registration process that are working with the registration team. And these profiles would replace the traditional access methods and user roles that we currently have in the system, and these profiles would be based on what they needed to do within the system. So how much -- and taking into account things like how much information is necessary to ensure the identity, what the structure of the company is, what information can they see and not see, and their relationship with the organization such as monitoring the compliance interactions or interactions with customer support.

And as we talked about, using commercial data sources, we would be able to use the information from that potentially to help us slice and dice and create the right kind of user profiles.

And the next recommendation is to implement audits and take steps to penalize and publicize fraudulent uses of the E-Verify system. E-Verify's Monitoring and Compliance Branch is charged with ensuring that E-Verify is used properly and ensuring the integrity of the system. So

as you can see on the slide, the Monitoring Branch is focusing on identifying non-compliant uses of the system, both electronic and manual analysis, and then referring those incidents to the Compliance Branch, which will carry out escalating series of employer contacts that include compliance assistance through letters, calls, emails meant to educate the employer and alert them to potential misuses. And then if there are repeat and severe incidents, they can escalate as necessary to desk reviews or site visits, and we do work with ICE and DOJ's OSC Office, as necessary, to refer cases.

We also wanted to point out some of the additional enhancements that have come out of our registration reengineering project, and the focus really is on increased usability and improved customer experience through the registration process and through using the E-Verify program. So we hope that our new registration process will be a more streamlined process that is logically flowed, and then also that things like a side navigation bar will tell people where they are within the process. Currently, they just go through the process without knowing the next steps. So we're hoping this will

provide a better user experience.

In conclusion, as you can see, many of our current efforts are aligned with the DPIAC's recommendations. So we were happy to see that we were both heading in the same direction and that we've definitely used DPIAC's recommendations to help drive our registration reengineering effort, and also our look at user profiles and monitoring and compliance.

So our goal has been to ensure that we know our customers from both a customer service and security standpoint, to improve our process and user experience, enhance security and improve information quality in our system. Protecting personal privacy and ensuring data integrity have been a main focus of the registration team, and we look forward to continuing to interact with DPIAC on that as we move forward.

And we welcome any questions.

MR. BEALES: Thank you. Could you -- you mentioned in that last slide that the scheduled rollout of the first stages of the program are at the end of the year. What's part of the first stages, and what's the timeline for other stages?

MR. MAYHEW: Sure. The first stages we are looking at hopefully December 2009, and part of that would be enhancing some of the usability elements, like Liz said, adding a lot more intuitive usability so that people are able to get through the registration process.

Second, adding the roles and profiles, hopefully, at least the start of it so that we can start to limit the actual use rights of some of our users.

The third would be, and the big one, is the company validation. That relies on a procurement of a third-party data source, which we are actively pursuing. Whether we are able to pursue that and implement that in December or whether we would have our next available release sometime in 2010 is up to debate, but we are moving aggressively towards that because that seems to be, from the recommendations you've given and from the work we've done, one of the main concerns that we're looking to address.

MR. BEALES: All right. Thank you.

John Sabo.

MR. SABO: Well, you really compressed -- I mean, it's great to see that our recommendations are

aligned and you're really working through them. It sounds like you're putting a lot of effort into it. But you really compressed a lot into 10 minutes. So I think hopefully we'll have an opportunity for -- we had an ad hoc subcommittee which developed the recommendations, and hopefully we'll have an opportunity to work with you on more details. There isn't a huge amount of time.

But having said that, a couple of things struck me. One is this continuous -- and with the new Obama administration's focus on government efficiency and government transparency, a new CTO, a whole focus on getting through some of the barriers, what strikes me is the continuous problem where one agency under a Congressional mandate to implement a program -- now this is now a voluntary program, the inability to go across government barriers.

I mean, you have the IRS code which prohibits the use of the EIN for non-tax purposes, but you have companies who are voluntarily, if I'm reading this correct, making use of this program. So you have one barrier, and then you have a voluntary use of a program which cuts across another agency. And it just strikes me -- and other

agencies are looking at similar employer uses, similar access to employers. Right outside this room today there's a whole convention, it appears, of Social Security disability companies who support those who have problems with getting their disability benefits, and it's a whole other area where other agencies like SSA are grappling with the same problem.

How do you identify an institution which has the right to support a claimant, in this case for disability benefits, very analogous to what you're doing? They're trying to determine employment. You're trying to work with employment eligibility.

So the same problems are going across agency after agency after agency, and your use of the word "profile" was interesting. In the standards world, we have standards. And often to implement them, you develop a profile, which is a particular instantiation of that standard. And I guess my point here would be to think about or overcoming some of those barriers across institutions and maybe using the administration's new focus on across-agency implementations and try to develop a cross-agency profile that would address this issue, which

is you've got a corporate entity, an employer, and it may be a single practitioner or a corporation, a big company, and there are multiple governmental uses for them to identify themselves. We're not dealing with personal information. We're dealing with corporate information. And within those corporations you've got multiple users who have roles. I think your approach to role-based is right on track, perfect, and there are new developments in authorization now. Role-based access is migrating to context-based access controls, which rolls one component.

So there's a lot going on in your presentation, but I think you need to be -- you should be commended for what you're doing, which is looking at it very structurally. But my big concern is time. I mean, we have, as you're pointing out, new uses coming online every day, and it sounds like we still don't have the controls in place that would address some of the concerns, many of the concerns of the Committee.

So I guess I'm rambling on, but I think it's great that you're moving in this direction. You seem to be focusing properly on some of the structural things that we raised. But I'm still concerned that -- and it's not,

again, a DHS issue per se, but it ties into the bigger issue of how do you come up with a secure, privacy-aware, effective system for identifying employers whose employees have access to very sensitive information. And I would hope that there's some way to reach across boundaries on this.

So I guess I rambled on enough, but hopefully we'll have a chance to work with you on some of the details of what you're doing.

MR. MAYHEW: Yeah. I mean, we appreciate definitely the thoughts, and we definitely would welcome the chance to speak to the ad hoc committee a little bit more in-depth about the efforts we're taking.

Something I left out that Kathy mentioned was part of what we're also looking to doing in the registration process and the validating of company information is not only starting from today forward all new registrants, but going back to all the 110,000 -- 140,000, I think, MOUs and 400,000 worksites that there are now and cleaning the data that we have so that we will know our customers based on third-party data sources, based on monitoring compliance and outreach, all our customers, and

have validated them going forward, because that's an important point, that we don't want to fix it just for everybody from today forward but fix it so that we have a uniform standard that we can look to and know that all those customers have been validated.

MR. BEALES: Could I ask just one more -- one timing question about another piece of this, and that's the monitoring. What's the timing for that to be online and in place?

MS. LOTSPEICH: Sure, I'll answer that question. We're looking in the June timeframe to be able to access what we call internally the Compliance Tracking and Management System. And actually, the SORN and the PIA should be up probably in the next couple of weeks. So I would direct the Committee to looking at that to get more in-depth information about how we've structured that program.

And what we're doing and what we'll be able to do using this system is to do some routine reviews of different indicators in the transaction database that we have where we think there's a hint of non-compliance, and we would have monitors look at these data, draw some

conclusions, and if they thought that it was enough information that warranted more compliance assistance and more review, then we would use this what we call CTMS, Compliance Tracking Management System, to develop a case, and then we would begin to work with an employer and start to try to correct that behavior, and/or refer it to an appropriate agency such as Immigration and Customs Enforcement or the Office of Special Counsel at the Department of Justice.

MR. BEALES: Joanne McNabb?

MS. MCNABB: Thank you very much. I have two areas of questions. One is regarding how this employer verification procedure will work for small employers, I mean very small employers, individuals who are employers who are not going to show up in any kind of database.

MS. DENNISON: Sure. Through some of our proof of concepts of different third-party data providers, we've worked with them to try to identify what would happen if someone wasn't in their database or what kind of data they have on very small businesses. So we've actually found that they have a good deal of data on very small businesses that we would have expected them not to have. So that was

a surprising and pleasing thing to see.

But as Mike pointed out when we went through the slides, if during that validation point that person isn't found in our third-party commercial database, we wouldn't deny them registration based on that, and what we would do is we would have some note in our system that said it didn't match up, and we would be able to follow up with them, which is an outbound call to say we saw you registered, get a little more information on them to ensure that they are a company, or we would work to try to identify instances that are individual people and then have a process set up from there in terms of identifying them as a business.

So we wouldn't deny registration based on someone not being in a third-party database, and we're trying to work out the algorithms and what would happen from there when those instances occurred.

MS. MCNABB: So you'd monitor something like they're processing an awful lot of potential new hires through this for their size?

MS. DENNISON: Sure. Exactly. That's exactly what we're looking to do, is to do that validation check,

find out if they did match up with a company in the database, and if not, then we would make sure that we monitored their usage to make sure it fell in line with what kind of company they really are.

MR. MAYHEW: And to follow up on what Liz is saying, one of the things that we're thinking of in terms of our monitoring and compliance is if a certain company says they hire 25 people a year, and then our monitoring analysts will be looking and see that they've run 100 queries in a particular month, that would engender a phone call to say we noticed some anomalies in how you're using the system, we'd like to follow up.

MS. DENNISON: Right, and it might be just misinformation, typed information during the registration process, or it could be something that would require education on our part to the employer. So we would make sure we monitored that appropriately.

MR. BEALES: But the structure here is the registrant gets access right away, and then we wait and see if they're doing things that look suspicious. Is that -- am I understanding it right?

MR. MAYHEW: Yeah. Essentially, the registrant

would get access right away because if we were using a third-party data source, we wouldn't necessarily want to deny because the third-party data source isn't perfect. But these would be flagged very quickly, and if it was identified as a risky company because they didn't match against this third-party data source on any of the information they provided, we would hope to give a phone call within the next day, or within the next couple of days, so that we don't let them use the system for a week or two weeks. Hopefully the follow-up would be very quickly, and we're working on the internal controls to make sure that happens.

MS. MCNABB: And what exactly would you be asking them? "Oh, yeah, I'm fine." I mean, what are you going to be able to get from a phone call?

MR. MAYHEW: We would essentially -- sure. I mean, it's a fair question. We would be following up to say, essentially, this is the government calling, we know that you registered, we are looking to provide assistance and education on --

MS. MCNABB: And we'll be watching you?

MR. MAYHEW: Not in so many words, but yes.

MS. DENNISON: And we would also check to make sure if maybe they didn't match up against the database because of a typo or misinformation, or if they're a small piece of a bigger organization that actually is in the database that we can match up in some way, so then we can put them into a more trusted employer profile and kind of build from there.

MR. BEALES: Well, let me ask about a scenario that happened in one of the big data breaches, and that was ChoicePoint. And that is, I mean, they didn't ping, but had they pinged the database, what they would have found was, yeah, this is a phone number and it's a valid phone number, and it's a Kinko's that they're using as their business address and phone number. I mean, yeah, there's a possibility of errors in the database, but there's also a different explanation that's possible.

MR. MAYHEW: No. I mean, it's a fair point, and if it is a Kinko's, we would hopefully call that Kinko's the day after they registered, or two days after, and the Kinko's would answer and say we never registered, and we would shut their access off, because if we call and the person says that they've never registered as an

employer, that would be enough justification for us to close that access off. But your point is well taken, and it's something, truthfully, we would have to work through.

MR. BEALES: Is there not a way to delay that access in that case while this verification is happening, as opposed to you get access to do however much damage you can do, and then we'll cut you off as quickly as possible?

MR. MAYHEW: Truthfully, it's something we can consider, and it's definitely a good recommendation. Because we are not entirely familiar with these third-party data sources, we thought it was best to not shut off access. But the idea of delaying access for a couple of days and giving us a chance to follow up makes a lot of sense, and it could be something we look at, changing what we presented to you to allow for that.

MS. MCNABB: And then I have a question. Are you through on that one? If you want to continue that one, Howard, go ahead. Okay.

So the other whole area of concern about this system is the higher level of authentication accuracy of non-U.S. citizens compared to U.S. citizens and residents who are being verified against the Social Security

database, which is much less rigorous a comparison than the comparison on the alien side. So there's, I would think, a trend to push the fraud, the individual applicant fraud, not your customer fraud but your fodder and victim fraud over to that side.

So I'd be interested in hearing how you're considering that and what sort of measures you might have in place.

MS. LOTSPEICH: To make sure I understand correctly, so you're saying that because there's more thorough review of non-citizens, and what you mean by that and what I understand that to mean is that we not only check the SSA but in the case of a non-citizen we also ask for a green card, EAD, et cetera, et cetera?

MS. MCNABB: Yes.

MS. LOTSPEICH: Okay. So then from there, then what you're saying is that there might be more fraud than people trying to present as U.S. citizens in the system in order to avoid --

MS. MCNABB: And presenting a fraudulently acquired Social Security number.

MS. LOTSPEICH: Okay. Good, I understand. I

have an answer, too. What we're looking at right now is instances in our system where we see that the Social Security number, the citizenship status, in this case U.S. citizen, the date of birth and the name match and come out as employment authorized and are being used multiple times within the system. And we are seeing instances of this. We're able to develop reports that find these types of patterns, and we're looking at those very carefully because there are plausible circumstances where an individual could have more than one place of employment within a certain given time, and then there's other instances where it's not so plausible, where you would have 10 or 15 jobs in six or seven states within a six-month period.

And so what we're doing now is we're reviewing these and trying to find these patterns and trying to find these identities that are being compromised or that appear to be compromised and referring those, as necessary, to the appropriate authorities, and in this case we are working with ICE at this point in time. But we're also working -- and actually I'll turn it over to Mike to talk a little bit about another identity theft type of protection program that we're looking to pilot later on this year.

MR. MAYHEW: Sure. One of the ideas that we're tossing around, we're honing our monitoring processes so that we're able to identify these instances. But as you pointed out, one of the types of fraud that's perpetrated is non-citizens posing as citizens, getting a Social --

MS. MCNABB: Or citizens posing as other citizens.

MR. MAYHEW: Exactly, getting a Social Security number, getting a driver's license, and then being able to work because there is a lower standard. So as our monitoring group identifies these instances, and as Kathy mentioned, multiple instances across multiple states where it's no longer plausible, we are batting around the idea of locking that particular Social Security number in the system and essentially forcing a Social Security TNC and making that person go in to a Social Security field office.

We are working with Social Security on that idea, but we truthfully have to get our monitoring up to speed so that we are able to confidently make that assertion and confidently lock the Social Security number with some justification. But it is a way that our Monitoring Compliance Branch can take a proactive action to

defend the integrity of the system, which I think we both agree is very important.

MS. MCNABB: Yeah, and that -- I would encourage you to be moving as rapidly as possible on that side because I would think it's going to become more of a problem as we go forward.

MR. MAYHEW: Sure.

MR. BEALES: Neville Pattinson.

MR. PATTINSON: Thank you, Howard.

First of all, great to see our recommendations taken on board and worked on. Terrific. Thank you for making us feel valuable.

So first of all, in a validating employer, I think you have some good work going on there with third-party databases. It's very encouraging.

Validating employees I think is an area I just want to explore a little bit on some of the proposed techniques that you're looking at there. I have three questions that are quite simple.

The first one is, really, is there any linkage from the MOU that's signed by the applying organization to email addresses? You talked about the use of email

addresses here. So is there a domain name check, an email verification from the MOU to whatever the registrants are enrolling in when they enroll? If they're using a Hotmail account or a Yahoo account, then that doesn't kind of give you a lot of confidence that there's really an organization potentially behind there. So that's the first question, is there a linkage all the way through perhaps to the user name, or maybe using email addresses as the user name?

The second one is really about usage, and looking at your proposed authentication methods, certainly my recommendation and my encouragement would be that you're authenticating every time somebody is coming on through that third channel, that back channel. So even though you're using a username and password after you've enrolled, you still are challenged for that extra piece of authentication material, maybe not just biographical but certainly a code transmitted through fax or SNS, whatever you're proposing. Every time they log in, they're challenged for that as a real authentication every time, and if that's part of your scope, and when those trials or pilots are going to be done.

The third simple question was really one I

didn’t see in the presentation regarding the imaging tool. We discussed that some time ago, where you’re able to transmit and display the alien file picture, I think it was from the green card. Is that picture obscurified in any way so that it can’t just be printed and made into another card or whatever? Because you’re giving the real facial image that’s on that card. So we saw a vulnerability there of that picture being delivered in a form that could be beautifully reproduced on another fraudulent card.

So three little questions. See if you can give some answers, please.

MR. MAYHEW: Well, I can answer the third question first. The photo will be -- we’re going to institute photo protections on the photo in a bill that’s coming out in September. So we took the recommendation, and it’s always been a concern of ours, and we’re going to implement that very soon.

The first question, is there a linkage from the essentially email address validation? It’s truthfully something we haven’t looked too much into, and it’s a good idea. The problem is, as was mentioned earlier, there’s a lot of small businesses that use our program which might

have a Hotmail address. It might not have an AcmeCorporation.com email address. So it's something I think we could take back and look into, but it's definitely a good idea.

MS. DENNISON: And as we look at using third-party data to also help us understand our customers more, we can actually compare the email addresses that they have on file for the company versus what the person gave during the registration process. So that can help with monitoring as well and looking at more validation through the email addresses. And what we talked about with validating, sending them an email and having them log out and log back into the system, was our first step into that. But your recommendations to have that be even more of a rigorous process are definitely well taken, and we'll take that back.

MR. MAYHEW: And I think to your second question, an additional token as opposed to just username and password, it's a very good point. We run the risk of, I think, because this is a big system that's constantly growing, and because adding additional complexity might not be understandable to a small business in Idaho or something

like that, adding tokens, we have looked at the technology. We will continue to look at the technology to see if there's additional authentication that we can do on a continuing basis of the user.

As Liz mentioned, we're looking at doing individual authentication of the individual users when they register or are added as a user. But I think an important point that we have kind of thought through is that our registration process should not be a one-time conversation at the beginning. It should be a continuing conversation that we have with our user and with the employer to continually update their information, to continually verify that they are still a company and still existing.

And one of the ideas that we have had with using third-party commercial data is that we would like them to inform us if a particular company has gone out of business according to public records so that we are constantly looking to see if this company should still be using it, and if they shouldn't, shut off that access so that it isn't a user who has a username and password and his company went out of business but he still has an active account in the system.

So I think an important point of the continuing conversation of registration is something that we're really looking to implement because it will add security to the system and the system's use.

MR. BEALES: Kirk Herath?

MR. HERATH: Thank you. I want to compliment you. In four and a half, five years, I think this probably is the best, singularly the best presentation I've ever listened to. I mean, for the first time, I think we see actually our recommendations sort of in operation, which is just very gratifying because all of us, you know, we don't get paid a lot of money to do this.

[Laughter.]

MR. HERATH: So it's fun to see our work come to some fruition. So I do compliment you on that.

Obviously, this is not a perfect system that you've designed. Nothing sort of built by man will ever be a perfect system. So my colleagues, most of whom are far more expert in security matters, I think have pointed out some fairly common problems with any large database that has a lot of disparate customers who you don't know and who you don't interact with in a personal sense.

I would recommend that -- maybe Joanne can help you -- the California Department of Motor Vehicles actually has some phenomenal standards from a user perspective that they require people accessing their database to comply with. They audit against it. Honestly, it's one of these under-looked security -- I mean, it actually has --

MS. MCNABB: Like an insurance company.

MR. HERATH: Right. So like an insurance company, we have a lot of people who access these records. It actually -- we actually have a time-out on our desktops and our laptops basically predicated on that, on those guidelines. So it drives behavior for a Fortune 100 company, and it's very simple, and they do a lot of the same things you do. They have a "trust but verify" model. They look for somebody who is usually hitting it once or twice a week, hitting it 200 or 300 times a week.

So Howard actually asked several questions that I was going to ask. The one question I have on transparency is, so I assume you'll be tracking as you monitor the use, you'll be tracking the investigations and you'll be developing metrics out of that? And will you be transparent with everybody about what you're finding and

how you're fixing them?

So how many people are you, you know, shutting down? How many people are you passing over to law enforcement?

MS. LOTSPEICH: Well, I can't speak for ICE or OSC in terms of once a case is referred, how that investigation goes or what the outcome of that is. That would be in their purview to be transparent on those particular cases. However, we can and do track referrals, and we do plan to provide metrics on how many employers that we touch, the nature of the types of violations that we saw, the methods we used for follow-up. So, yes, this is something that -- and that's one of the reasons that we needed a system, really, the CTMS system that I spoke of earlier. We took some time to develop that in terms of what our needs would be for storage of information, sorting. And so, yes, that is something that we will be doing.

MR. HERATH: Okay. And my final comment is don't let the perfect be the enemy of the good. So just keep evolving this thing as you get feedback from your customers, as you get feedback from us and others in the

public. Your strive should be perfection. You'll never get there, but I think this is a very, very good discussion. Thank you.

MR. BEALES: Ramon.

DR. BARQUIN: Just a quick question. In our Subcommittee we've been looking at some of the architectural issues related to privacy, and there is at USCIS an effort called PCQS, Person-Centric Query. Are you involved with it at all?

MS. LOTSPEICH: Yes, we are.

DR. BARQUIN: Okay.

MS. LOTSPEICH: A one-word answer. Do you want me to expand on that?

DR. BARQUIN: Please.

MS. LOTSPEICH: PCQS. We do -- we work -- there's a -- if a person does not become authorized immediately with our system, and this is in the case of a non-citizen, then we ask for additional information. So we do work with the PCQS system. We have a dedicated staff. We call them status verifiers. And so they've been able to work with that system to help home in on an answer for whether or not someone is work authorized.

DR. BARQUIN: Is this direct online work with an interconnected E-Verify database, access through PCQS, and vice versa?

MS. LOTSPEICH: On behalf of government staff, not the employer.

DR. BARQUIN: Yes.

MS. LOTSPEICH: It's all behind the scenes.

DR. BARQUIN: Okay.

MS. LOTSPEICH: So, yes, we do, and they're a trained group of individuals not only on PCQS but generally on -- a lot of them are former adjudicators. So these are sort of like the guts of the USCIS type of work, looking at status and changes in status.

MR. BEALES: Joe Alhadeff?

MR. ALHADEFF: Thank you. I guess I had one question about the external database, whichever one it turns out to be that you guys will end up dealing with, and then one question which kind of went to some of the monitoring issues.

So the question I had with the database was you talked about, what happens if there's a keying error and it doesn't match correctly with the database? Is part of the

agreement that you're going to be able to write with this vendor, though, that if the database has errors, they'll do a correction? Because otherwise you'll have sequential mismatching that continues to occur. So you need to make sure that the source data actually becomes accurate if there's an error in the source data.

MS. DENNISON: We've definitely talked to them about that as we've been working through proof of concepts, and they are definitely -- they have a whole process in place, many of them that look at updating their records frequently and using the information that they potentially could get from us to update their own records. And they have a manual system past their automated point that would look at if there's just a slight typographical mismatch, manually checking and making sure that we're not sending a non-response or a non-match back when it's actually a match.

So they definitely have that in place, and we would work with them to ensure that we wouldn't have multiple mismatches back and forth, back and forth, because of one data mistake. So that's definitely something we're keeping in mind and working with them on.

MR. ALHADEFF: Okay. And then the question related on your slide which had the monitoring, and you're looking at behaviors as one of the ways to measure monitoring, and I guess I was just wondering whether there were also spot audits to actually measure misuse of the system or to find occasional misuse of the system, because you might not actually have a behavior that is elicited by that monitoring but you might find that there are misuses of the system through an occasional audit. And I guess that went to the concept which I guess is part of what the California system does, some level of audit against that so they can do checks on the proper use of the system even where no behavior is elicited that seems unusual.

MS. DENNISON: That spot audit, is that probed by when they see a transaction that looks different?

MR. ALHADEFF: I think it has to be kind of a neutral suggestion that there's a certain percentage of transactions that you're going to look at.

MS. DENNISON: Okay.

MR. ALHADEFF: I mean, because you're always going to investigate the ones that look a little funny. It's occasionally the ones that aren't funny that you find

out there are behaviors you have no idea that exist.

MR. MAYHEW: Yeah, I think it's an excellent point, and it kind of gets to what we were saying. We don't look at this as a company registering and then we leave them alone if they don't violate a behavior. We would like to check back in with companies. And part of the work the monitoring group is going to be doing is checking back in with the company on their actual data so that while they're monitoring on behaviors, they're also looking to monitor the system and see if there are anecdotal evidence or additional behaviors that should be added over time that we're not seeing. You know, this is a group that is starting. We have identified behaviors, but we will be adding more as they come along. But I think your point is well taken.

MS. LOTSPEICH: So, in other words, what you're saying is looking at employers who are not showing up in our reports that we're already looking at, so just a baseline of people who aren't coming in. I think that's something that we can examine.

MR. ALHADEFF: And, you know, even tremendously well-intentioned employers, I mean, there are some law

firms who are making very good money on I9 guidance at the moment, looking at exactly how to deploy these systems, because for a large organization, this isn't a straightforward process.

MS. LOTSPEICH: Thank you.

MR. BEALES: Lance Hoffman?

MR. LANCE HOFFMAN: First of all, a clothing note to Mike. I have to congratulate you on your sartorial --

MR. MAYHEW: Yeah, we dressed each other today.

[Laughter.]

MR. MAYHEW: Very good taste.

[Laughter.]

MR. LANCE HOFFMAN: Good taste.

I had the feeling listening to this whole discussion -- first of all, I want to echo Kirk's comments especially. It's nice to see our recommendations looked at and attempted to be responded to. This has more of a feel of we've got a long way to go, we don't know quite how we're going to do it, here's how we think we're going to do it, and then I hear a number of people around the table saying have you considered this, have you considered that,

blah blah blah.

I'm wondering if you have a process in place in general to do this sort of thing, or do you just sort of sit around a room and say, hey, what should we do? We've got these problems. Because it strikes me this could be very useful if you don't have them, and if you do, it would be a good example for perhaps other DHS components to exemplify.

MS. LOTSPEICH: Yes, I'll speak to that, and I want to say just a resounding thank you for your compliments to us, because we're a very flexible program with a lot of dedicated people. So it's nice to hear that our efforts are being well received.

We have a lot of forms and venues for making changes in our program and in our system, so I'll try to just gloss over them. One sort of more nuts and bolts and the core of it is we have our own internal CCB, our own change control board where we meet every other week with representatives from all the different branches within our division. So the privacy branch is there, the SAVE program, the E-Verify program, the monitoring compliance program, the special operations program, and everyone comes

to the table with what they want to be in the next release, and it's a very lively meeting that we have every two weeks. So it's more sort of a grassroots level business requirements, the people that are closest to the day to day work. So that's one layer.

A second layer is that we have an executive team within our division that we call the risk analysis group, and we work every other week and we get together, and we kind of play the "what if" game, and we think, well, what if this, what if that. We think what about legislation? How would we write a regulation? How would we handle registration? So we have sort of a policy think group internally.

We have a special projects division which has a direct line to the Deputy and our Chief, who, by the way, is sitting very quietly over there. He's taking notes. Our Chief is very supportive. He gives us a lot of flexibility. He brings a very nice, rigorous military approach to running an organization, but still allows a lot of freedom of thought.

And so we work with this risk team, and then we have, as I was saying, a special operations team which Mike

oversees, who is still young enough in government to not be cynical or jaded and works tirelessly every day coming up with new ideas to come up with ways to address such things as registration, identity fraud, all kinds of things like that, along with Liz Dennison, who is a key member on his team.

Now, that's just internally. Externally we have been very popular within the Bush administration, and it looks like we may also be very popular within the Obama administration as well. We benefit from having weekly briefings with the director of USCIS, so we get executive-level attention and people looking at us. We are able to get a lot of special attention from DHS Privacy in particular, and like I said, we have a privacy group.

And then we also have been a part of a lot of the major initiatives, both with the outgoing administration and the current administration. So we're kind of keyed into a lot of discussions on that level as well, and we also have an outreach branch and a 1-800 number that we get a lot of information from from the public, and those ideas also show up in our CCBs and in our various types of councils and meetings that we have.

So it's a model that's working well, but I would welcome more, and I think that we could really use your expertise in grappling with some of these issues here with the registration reengineering process as we move forward, because we're still in a requirement-setting phase.

MR. BEALES: Joanne, did you have another question?

MS. MCNABB: I'll ask them offline.

MR. BEALES: Okay. Well, I want to thank you very much. This has been a very helpful update. It is -- I'm glad we were able to be helpful, and it seems like you've been quite responsive to what we had to suggest, and that's very nice to see. So thank you, and we appreciate you being with us today.

We will now adjourn for lunch. The public portion of the meeting will reopen at two o'clock. There will be an administrative session for the Committee that is here at one o'clock. So for the Committee, we are on our own for lunch and need to be back for the administrative session. Since part of what -- the administrative session is here, yes.

Part of what's on the agenda for the administrative session is ethics briefing, so it would be unethical to be late. And so we need to be back here by one o'clock.

For members of the public, if you're interested in addressing the Committee, please sign up at the table outside. We would love to hear from you this afternoon after we hear from our Subcommittees. And I will see the Committee back here at one o'clock and the public back here at two o'clock. Thank you.

[Whereupon, at 12:20 p.m., a luncheon recess was taken, to reconvene at 2:00 p.m.]

A F T E R N O O N S E S S I O N

MS. LANDESBERG: If everyone will please take their seats, we'll get started and turn the meeting back over to Howard Beales.

MR. BEALES: All right. Thank you very much. We will turn now to our Subcommittee reports. I'd ask everybody to please make sure your cell phones are turned off, and if you want to speak to the Subcommittee, or speak to the Committee at the end of the day, please sign up at the table outside, and we will turn to public comments whenever we're done with our Subcommittee reports.

So we will start with the Subcommittee reports. I guess we will begin with Privacy Architecture, if there is a report from Privacy Architecture. Joanne McNabb.

SUBCOMMITTEE UPDATES

MS. MCNABB: We have nothing to report.

MR. BEALES: Well, thank you.

[Laughter.]

MR. BEALES: How about the Data Integrity and Information Protection Subcommittee? Charles and Ramon.

DR. BARQUIN: I will take the first stab given the alphabetical order of the Co-Chairs. We have been working thoughtfully, I must say, with the Privacy Office, trying to address the specific issues of dealing with the privacy challenges of SOA, service-oriented architecture, and I think we are now on a path to actually having a number of meetings with the SOA experts at the Department level and some of the components from which we should be digesting and developing specific plans and recommendations, and Charles can add all the real meat to that.

DR. PALMER: Great. Thank you, Ramon.

Clearly we've taken a little time on this, you may have noticed. There's some good reasons for that, some of which is if you think about going into the future, if you don't get SOA right, you're in real trouble when the

cloud comes. If you don't get SOA right, some of the other things that are happening that people are already selling to the government aren't going to be right either.

And so getting this right has been very, very, very important, and as a result we've had to have several conversations with our colleagues at the Privacy Office to make sure that what we make our recommendations based upon is actually something useful to be based upon. We can't just assume that the answer is between the two points. We have to know the answers to get from here to there.

And so, yes, it has taken a while, but I think we are well -- as Ramon says, we are on our track now, and I think we have a good direction, and it's going to be up to us to make sure that we drive this through and make sure we have these meetings. Otherwise, it won't be very good going forward. So I think we're there.

MR. BEALES: All right. Thank you very much.

Our third Subcommittee actually has a matter on the agenda, and that is a draft white paper on information-sharing and access agreements that is still available, I think, outside for anybody in the public who wants one. I really want to thank David Hoffman and Richard Purcell, who

is not with us today, for their tremendous work on this document. I know it's been a long and involved effort, and I really want to thank you for it and ask David to please present the document, and then we'll proceed with a discussion.

MR. DAVID HOFFMAN: Thank you, Mr. Chair. I would also like to pass along those thanks because the rest of the Subcommittee really made the work that Richard and I did so much easier by the tremendous amount of work that they did and the thoughtful analysis. And also I'd like to thank the support that we received from the staff, specifically Toby Levin and Martha Landesberg, which was tremendous in helping us to be able to do the job that we had in front of us.

The paper that you have a draft of and that I will be making a recommendation for us to vote to adopt and go final on is, as we noted at the last Committee meeting and in the report out from the Subcommittee, focused on addressing the issue of what controls should be put in place within the information sharing environment in situations where DHS is being requested to share specific information.

The recommendations in this document split out into five different categories and are captured on pages two and three. First there's recommendations specifically to categories of oversight that would be required, the establishment of an information sharing review board, and direction to be provided specifically by the Secretary.

The second is then the creation of an information sharing threshold analysis with an expectation that when sharing is going to be completed, there would be a template analysis document that would specify a number of questions that need to be asked about whether that information is going to be shared appropriately and what controls are going to be in place for the sharing and the use of the information.

Depending upon the information that results from that threshold analysis, that would bring us to the third step in our recommendations, which are the completion of sharing agreements if there's going to be sharing of information outside of an individual component. So from one DHS component to another component, or with DHS to another entity. The idea is that the obligations for how the data should be used, processed and protected should be

captured in an agreement with specific understanding of what the provisions should be in the agreement.

Then the fourth part of the recommendations go to the communications out to the folks within DHS and the folks with whom DHS normally works to communicate that these processes are important and the controls that they're supposed to put in place.

And then the fifth category of the recommendations is to put in place a standard process to be able to go and to audit and to understand whether the processes are being followed and are being implemented to actually protect the data.

That being said, I have received a few comments during the last 24 hours which I think are important enough to make us -- to make me recommend a few edits to the document to make some points specifically clear. So for those who would like, I would recommend this is a good time to grab your pen. I have specific drafting edits that I will propose, and then we can take these in whole for passing the document, or in discussion we can discuss specific provisions, either these edits or other provisions that people take issue with.

The first proposed edit would be on page one in the last paragraph in the sentence, the second sentence of the last paragraph, starting with “It is critical.” That sentence would be continued. And so it would now say, “It is critical that DHS establish specific policies and practices to govern broad information sharing to ensure that personal data is respected and protected,” and then it would extend to say, “for sharing within DHS and with organizations external to DHS,” just to make clear that it applies to both types of sharing. Does anyone want me to pause or to say that again?

DR. ANTON: David, should that ensure be with an “e” or an “i”? Now that we’re there.

MR. DAVID HOFFMAN: I believe that should be with an “e”.

DR. ANTON: Thank you.

MR. DAVID HOFFMAN: So “ensure.”

MS. MCNABB: Organizations or agencies?

MR. DAVID HOFFMAN: Organizations, because it could be broader than a specific agency, especially if it’s a state and local organization.

MS. MCNABB: So should it be government that

we're talking about, right? We're talking about government entities, though, right?

MR. DAVID HOFFMAN: No, it could be broader than that, especially at the state and local level external to DHS. It's intended to be broader than that.

MS. MCNABB: Private sector.

MR. DAVID HOFFMAN: Could be, or NGOs.

Any other questions about the first edit?

[No response.]

MR. DAVID HOFFMAN: Moving to the second edit on page two, in the recommendation section near the bottom, Threshold Analysis, first bullet point, we would add an additional sentence. That sentence would say, "Also, the DHS Privacy Office should include a question in the template Privacy Impact Assessment to trigger the determination of whether an ISTA is necessary." The reason for this edit is to make clear that this should integrate with the already well functioning process set up to require Privacy Impact Assessments to be created and allow that to be a trigger with a question asking whether sharing, information sharing is happening, to then trigger in to understand that the threshold analysis should be completed.

MS. MCNABB: Can you read it one more time?

MR. DAVID HOFFMAN: Certainly. "Also, the DHS Privacy Office should include a question in the template Privacy Impact Assessment to trigger the determination of whether an ISTA is necessary."

Other questions or comments on the second edit?

[No response.]

MR. DAVID HOFFMAN: Okay. Moving to the third edit, this is now on page five. It is in section two of this portion of the paper where it says "Review Information Threshold Analysis." It is in the first paragraph, and it would be to insert a penultimate sentence in that paragraph. So just before where it says "the ISTA process," it would now say, "One important mechanism for the component CPO to become aware of the sharing request should be inclusion of a question in the template DHS Privacy Impact Assessment." It's the same substantive comment as the last edit.

DR. ANTON: I would just note that some of the substance seems to be missing in the second version of that. So in the previous time you said something about the question to trigger, and that phrasing was missing from

this sentence, I believe.

MR. DAVID HOFFMAN: So we could do that by saying -- I wasn't including that since that will already have been in earlier, but I can repeat it here if you would like to say, "The question in the template DHS Privacy Impact Assessment to determine whether a privacy" --

DR. ANTON: I think it's the same wording you had before, but I think it is valuable to not leave it up to interpretation if someone did not read the first part of it.

MR. DAVID HOFFMAN: Okay. So that would then say "to trigger the determination of whether an ISTA is necessary." Any questions or comments about that edit?

[No response.]

MR. DAVID HOFFMAN: I move to the next edit with some trepidation for the conversation that could result. This would be the fourth edit at the end of that same paragraph. There's been a recommendation to include a period at the end of the sentence. I'm open to debate.

The next edit is on page six at the bottom of the page under the header "Privacy Management Controls." This would be to delete the first sentence and replace that

sentence with the following sentence: “Integrating privacy into information sharing requires behavioral controls and oversight to ensure personal information is disclosed and used appropriately.”

This is in response to a comment that the phraseology that was in there before of maintaining the privacy of personal information might confuse some readers to think that we are just talking about confidentiality and not talking about controls around the use of the information. Comments or questions on that edit?

MR. BEALES: What was the phrase at the end? “Requires behavioral controls and oversight to ensure personal information” --

MR. DAVID HOFFMAN: “Is disclosed and used appropriately.”

Okay. Then the last edit or proposed edit is on page eight at the beginning of section three where it says “Documentation, Information Sharing and Access Agreements.” This would -- this edit would delete at the beginning of the first paragraph the phrase “after, if the ISRB.” It would then delete “approves an ISTA” and instead would replace that with the following sentence, and I’ll read

from the beginning of the sentence.

"If the ISRB determines from the ISTA that personal data will be shared outside of the specific DHS component, then the component Privacy Officer should ensure an information sharing and access agreement is completed." This edit is an attempt to solve two issues, number one, to make clear that if information is being shared but none of it is personal data, that it does not require then necessarily an agreement; the second thing that it's attempting to solve is to state that our recommendation is not requiring that when an individual DHS component shares information within itself, that it needs to create an agreement with itself. There may be situations where DHS may want to do that, but it's not clear to me that it's obvious enough that we ought to be making that recommendation to the Department.

Any questions about that specific edit?

[No response.]

MR. DAVID HOFFMAN: With that, Mr. Chair, I would leave it open to discussion of the paper if anyone has comments.

MR. BEALES: All right. Mary Ellen, did you

have a comment? We would love to hear from you.

MS. CALLAHAN: Thank you very much, David, and thank you very much for the hard work.

I wanted to talk first about the first and last edits that you had. I wanted to -- you talk about the one DHS policy, but I wanted to explain to you that, consistent with the Privacy Act, you are capable of sharing within an agency without having to do these steps, without having to do any of the analyses. Within DHS, you know that we are one DHS. And so what I wanted to raise to you is that the first recommendation and the last recommendation have recommended rather significant hurdles that are not within the current DHS framework.

As you know, we have an interim rule related to this. And so I wanted to be very clear where the Department policy is on this, and to the extent that that is your recommendation, I wanted you to know that it is unlikely that the interim rule would change with regard to information sharing between the components.

MR. DAVID HOFFMAN: Thank you very much for that. I think I'd be interested in discussion from members of the Committee about whether we should make any further

modifications. I think the concern that was expressed would be we could envision situations where, for example, since DHS, its individual components have such varied responsibilities, where, for example, CBP or TSA could request information, let's say, from FEMA, and it seemed difficult to recommend that it was less important to put some of these controls in place in those situations than it would be for sharing between DHS and other Federal agencies. And that's the reason for the inclusion.

MS. CALLAHAN: Fair enough, and that's a fair example. But what I wanted to remind you guys was that the components will still have to be governed by their Privacy Act statement, including the routine uses and the need to know and who has access to it.

So I would posit that those types of issues are already addressed in the ways that the components share between each other because of the restrictions that they have, separate and apart from information sharing between different agencies. And the information sharing environment and between the different agencies is trying to address, yes, you may have a routine use or you may have an ability to share it, but at the same time you may have

different agencies and different access points.

And so I only wanted to highlight that I think that your CBP-FEMA sharing example would have to meet the requirements. It wouldn't be an open pipe back and forth. It may be related to service-oriented architecture at some point, but isn't there yet.

But I just wanted to caution you about making the last recommendation in particular because as we attempt to systematize the Department and have everyone on equal footing, a recommendation to put in more controls between components may not be seen as useful.

Joanne? Howard, Joanne has a question.

MR. BEALES: Joanne, yes.

MS. MCNABB: Thank you. I wonder -- I take your point, and I'm sure that what we're trying to get at here is cases where there are potential issues of appropriateness of the sharing without some kind of controls between these components. How often do you think the routine use is interpreted very broadly in deciding what's allowed?

MS. CALLAHAN: I don't think in two months and five days I can answer that question.

MS. MCNABB: I think it's probably pretty often.

MS. CALLAHAN: It may or may not be, Joanne, actually. I think that there may be systems where -- for example, I was talking with my CBP colleague about TEXT, which is the CBP system that ICE often puts information in as well. So that would be an example where they would access it pretty broadly.

I think that instead of thinking about putting in controls within the different components, I think the better way to think about it is what's in the rest of the paper in terms of access and appropriateness of use and information. And as I said, the standard within the Department is on a need-to-know basis, and I believe that that is a standard that is always considered when the information is provided.

You can make your recommendation. I just wanted to explain to you how that recommendation may be seen because we're trying to make sure we systematize the information sharing within different agencies, because once it goes outside of DHS to -- I think it was Renard's point earlier -- that's when you have to rely on their good

representations about what they're doing with the information and the retention and so on.

MR. BEALES: So, Mary Ellen, your concern is about the recommendation, the oversight recommendation about ISAAs and the audit procedures recommendation?

MS. CALLAHAN: It was about the -- yes, essentially the -- and I'll have to admit, I was multi-tasking. But the first recommendation talks about the policies and procedures governing broad information sharing within DHS, and then he adds also outside DHS. And the last recommendation that I'm going to have to paraphrase, David, is essentially that we paper, we make sure that we paper sharing between the different components. Is that a fair --

MR. DAVID HOFFMAN: Yeah. What I heard you say was that the issue is applying these controls to sharing within the components, between the components.

MS. CALLAHAN: Between the components, yeah.

MR. DAVID HOFFMAN: Between the components within DHS. And so I think it's not necessarily a -- I mean, we can change the drafting. But I think if that's the substantive point, we should determine as a Committee

whether we want to recommend that controls be applied to sharing between the components.

I would state I think what we were going for here, just to relate back to the substance of it, is we were trying to make sure that the controls that were put in place would be close to minimal in a situation where people were already doing the work to understand how the data was going to be managed. So if people were already doing all of that work, then it would be fairly easy to complete everything. It's where that work wouldn't be done that it might impose a new requirement.

My expectation would be that as privacy continues to be systemized within DHS, these controls would be close to no burden. But I think that's an interesting question for discussion of whether there are specific controls in here that could be burdensome within the way the Department operates.

MS. CALLAHAN: Could you do me a favor, just to make sure that I'm not overstepping? And as I said, this is for your information. You can make the decision on the committee, but I wanted to explain to you what the thinking is on information sharing. Could you read me the last edit

that you have?

MR. DAVID HOFFMAN: Sure. I'll start from the beginning of the sentence, and it's on page eight of 10 under "Documentation, Information Sharing and Access Agreements."

"If the ISRB determines from the ISTA that personal data will be shared outside of the specific DHS component, then the component Privacy Officer should ensure an information sharing and access agreement is completed."

MS. CALLAHAN: Okay. Then I think my observations are relevant to that discussion.

MR. BEALES: Joanne?

MS. MCNABB: But, actually, John's tent was up first.

MR. BEALES: I'm trying to read the document and not paying attention to my Committee. All right, John, you can go first.

MR. SABO: My tent was up first.

MR. BEALES: I believe you.

MR. SABO: I guess related to that observation from Mary Ellen, I have a question on this. One of the issues we've had in the past is that exchanging information across agencies or subcomponents also relates to the

applications and the systems where the information is being shared. In some cases you're moving information from one system to another, and the other one is actually integrating that information or using contractor supported systems.

So my read of this, in part, which I thought was positive, is that -- and maybe it's inferred and not explicit -- is that it sort of says, look, I'm exchanging information in another component, but that component may use multiple systems or in turn may be sharing that information from their systems, and this would help establish the fact that those other external sharings are taking place. And so to that degree, I guess I'm not seeing it quite as -- I'm seeing it broader than maybe it has been intended. I don't know.

If that's the intention, that brings some visibility into clustering the various external uses of the information when you're transferring it from CBP to ICE, for example, and I didn't know if that was one of the intentions of the Subcommittee when you drafted this. But would that address the Privacy Officer's concern? In other words, you're not just sharing it with another component.

You're actually sharing it with the system, and the system may be sharing it with third- or fourth-party systems.

MR. DAVID HOFFMAN: Right. So to recapture that, I think you are articulating one of the concerns that we were trying to address, which is how do you make certain that the obligations that reside with the data flow with the data as they flow to a new party, whether that new party is inside DHS or outside of DHS? I will not -- I do not have the personal hubris to think that I could speak for Mary Ellen on whether that addresses her concern or not.

MS. CALLAHAN: Howard, can I speak again?

MR. BEALES: Yes, ma'am.

MS. CALLAHAN: Thank you. And I understand what your concerns are, and I think you stated it well, John. One of my colleagues here has reminded me that what I'm trying to do is just explain to you that under the Privacy Act, B(1), which identifies the agencies which can share it, DHS is defined as DHS, which I think most of you guys know that. And therefore it would be part of the routine uses in which the information would be shared within DHS.

So with that said, if you go and say, hey, DHS, ignore that one DHS approach with regard to information-sharing agreements, that is what I was saying that may be already addressed in the one DHS concept and the interim regulation which talks about it being one DHS.

With that said, John, you're right that the concern and the reason for the paper is that you want to make sure that the standards, the access, the rights that are associated with the data flow with the data once it comes outside of your control. The Department's policy is once it's outside of the Department is when the control and the concern may be. But that's right.

MR. BEALES: And the uses by other parts of DHS of information that came from one particular component, those would be addressed now in the SORNs and the PIAs of the user agency, whoever that might be.

MS. CALLAHAN: Exactly, Howard. So that would already be encompassed within the System of Records Notice because, remember, the routine use has to be spelled out whether it's by the agency for whom the Systems of Record Notice created it or for any other person in which it's shared. So it should already be within that concept.

MR. BEALES: Okay. So in a sense, in terms of our real concern that you document what's going on and how this is being used, you're saying that's there. Doing it through a formal information sharing agreement is not there, and that's what you're saying is not likely to be well received.

MS. CALLAHAN: I did not say that.

MS. MCNABB: I'm not sure that's accurate, or at least I understand that's accurate, that I understand that sharing from Component A to Component B in one DHS, that that is allowed as a routine use because it's within the same agency.

MS. CALLAHAN: Yes.

MS. MCNABB: But could it not still be the case that when Component A collected the information and said here are the specific uses, that the new specific use by Component B was not actually disclosed other than in that routine use which has gotten expanded by the creation of DHS?

MS. CALLAHAN: Joanne, I think to use your example, when I said, yes, that's correct, so using your CBP-FEMA example, FEMA says it has the information for

emergency purposes only, and CBP says, gosh, I'd love to see who is traveling on the southwest border during hurricanes. Well, that wouldn't be covered within the routine uses. So CBP would not be able to access --

MS. MCNABB: That would not be covered within the routine uses?

MS. CALLAHAN: The routine uses talk about sharing within the agency, but it's also for a specific purpose. So it's both agency-wide but also purpose driven. So you need to make sure -- if it's for law enforcement purposes, they may say that. That's pretty broad. But this emergency example would be one where probably the System of Records Notices for FEMA may say something like, you know, for health reasons, for this, for that, for making sure that people are safe and secure, that's why we collect this information. It would not be for -- I think ICE may be a better example. It would not be for checking immigration status, for example. And so that information could not go to ICE unless it was already within the articulated System of Records Notice. Does that make sense?

MS. MCNABB: Yeah, it makes sense. I just

didn’t know it worked like that.

MS. CALLAHAN: Hold on one sec.

MR. DAVID HOFFMAN: So while we’re paused, and I know other people had their tents up, but on this point I think -- let me offer another option which might solve this, which might be to say I think what we were trying to capture, and this is a point that Kirk Herath made repeatedly within our work, which is a very important point, that an agreement is effective for two different things: number one, to provide legal recourse if there is a breach of the agreement; but then the second thing is to put both parties on the same page as to what the obligations should be.

I think there’s a strong argument to be made that the first category there, providing legal recourse, is not particularly important when doing sharing within DHS just from component to component, and therefore what could potentially be an edit here that could solve this would be to say that the ISTA is still important within DHS when sharing from component to component.

But then if the ISRB were to determine that personal data is being shared between two components, then

there should be some formalized document that states what the controls are that should be -- the obligations that should be given with the data while not requiring specifically that it has to be a full agreement.

Mary Ellen, would that get more to the issue?

MS. CALLAHAN: To follow up on the thing we were talking about before, just to answer that, my description with Joanne was essentially accurate, that there's still the need-to-know basis.

Hey, Jim. How you doing?

Again, you guys can decide what you want. But to the extent that you're putting additional burdens on component-to-component sharing, that will not be useful is what I said, Howard, not well received.

MR. DAVID HOFFMAN: And I guess what I was trying to pursue there is I think the vision of the Subcommittee was that especially the ISTA should be viewed not as a burden but as a tool to help both of the parties better understand how to better protect the data and should actually be able to assist people in doing their jobs.

So if we were to rephrase this to remove the obligation of actually having to enter some sort of formal

agreement and have some sort of negotiation of what this agreement would look like, to instead have it be more the looking to go through that analysis to make sure that that's captured and that the parties are on the same -- the two parties who are sharing the information both are on the same page as to their obligations of how to protect the data, does that lessen the concern?

MR. HERATH: Yeah. Let me chime in here. So our intent was not to throw burdens on anyone. It's really more of a data governance, similar to what John said. It's knowing that Component A on a regular basis shares X type of information with Component B, who then we could ultimately track it that they then shared it with Component C. And if something untoward happens with it along the way, everybody understands their responsibilities and where it eventually -- so you'd probably come back to Component A in order to rectify it. I don't know.

So we're looking at this more as a data governance. We're not trying to restrict anything. It's just getting back to your transparency idea. It's simply saying where is the data, and follow the flows. And you don't know from a SORN where the data is. I mean,

conceptually it could be shared, but we don't know that it actually was shared and for what reasons.

I mean, FEMA is a perfect example. Katrina is a perfect example that we're trying to deal with here, where all this data went into the system and nobody knew where it ended up and what it was being used for. So it's a classic example of you didn't even know where to go for redress because you didn't know where the data was, you didn't know who had access to it.

MS. CALLAHAN: And I completely understand that, and I think the FEMA of 2005 is a different FEMA than 2009, I hope. And the concept of data governance obviously makes a lot of sense and is strongly supported. My only comment is that we've got a lot of information sharing conversations that are going on. In talking kind of sequentially on how to focus on these things, the way I read this paper was to talk about interagency sharing, and now with all the edits that have been proposed, it has become inter- and intra-agency sharing.

The ISRB and all of the mechanisms within DHS, and even the ISE Privacy Guidelines Committee that I serve on are all interagency sharing. And so that is where the

focus is. In terms of ISTA and having the process for intra-agency sharing, that is not the way it is currently being done in DHS. I do not envision that that will be the way it will be done.

So again, this is just a statement for your consideration in terms of how to think about what would be most useful for the Department in your recommendations.

MR. BEALES: Joe Alhadeff?

MR. ALHADEFF: For me, it's when I think of DHS and the complexity of DHS and its creation at a time of crisis, which was the bringing together of a lot of different, disparate groups, there is a reason to think about revisiting the concept of controls. If it was an entire agency designed from scratch where systems were designed to interoperate by definition, I think there'd be a much lower concern.

So for me, the concern is less on a per sharing basis than at a system-level basis to go back and see that the controls are actually in place so that you do have the appropriate issues, because SORNs and PIAs don't work on an ecosystem, which is what DHS is. They work on a system which might not even be an entire component but may be a

sub-part of that component.

So for me, what would be helpful in this document is if the overhead of a per sharing evaluation is problematic, a concept of going back and saying across the components we are going to see that these controls are instantiated in the proper way and that the limitations and the obligations are able to be transferred in an appropriate way, I think then you can wait and look for outliers because you've gone back and done the system review at the system level, which is a one-time, very painful exercise, but not a sequential every-time-you-ask-for-information exercise.

So I don't know if that would be a more constructive approach that might help look at some of these issues or not.

MS. CALLAHAN: I don't want to opine whether it's constructive or not. It's certainly not what this document is. I mean, you know, this document is information sharing and access, and I appreciate your perspective, Joe, and I appreciate the idea and the vision, and I think a lot of what you guys were talking about is taking place and will take place in the next whatever you

want to say, six months, 12 months, 24 months, as these things try to be implemented.

And I want you to understand I'm not saying that these aren't good ideas. I am just trying to have the Committee's recommendation be the most effective for the Department.

MR. BEALES: Lance.

MR. LANCE HOFFMAN: I'm wondering about the -- I take Joe's point about that SORNs and PIAs don't work in certain kinds of systems like we are in or may be getting into. I'm wondering about -- it seems to me it's more of a procedural issue here. What is the urgency of voting on this today versus going back one more time, waiting -- for example, would it helpful or not to have the Subcommittee look at this more to bring it back in three months, at the next meeting, where basically it's more or less the same material, let's say, but there has been more time to work with the new CPO, deciding which of these objections or concerns can be addressed and which cannot be addressed, which to go forward with?

I think it strikes me, but I defer to David and anybody else to get their opinion. I want to hear it.

This could be riper in three months, and I'm not talking about, as Mary Ellen said -- six months, 12 months, 24 months I think is too long. But three months is not that harmful to go back and look at things and see what could be, in essence, separated into controversial and non-controversial, and then decide what the Subcommittee and the Committee wants to do.

MS. CALLAHAN: In terms of the timing, and in terms of ripeness, I actually would respectfully disagree, Lance. Again, you guys can make your recommendation. My only issue is the intra-sharing, the intra-agency sharing. But I think the substance of this is actually really helpful, and you may put in intra-agency sharing, and the ISRB may just go and say thank you very much for ignoring that portion, right? I don't want you guys to be ignored. That's why I'm talking to you, to explain my position.

But with regard to the timeliness and the ripeness of this, the information sharing discussions are kind of going on now, so I think this would be really timely now. I don't want to force your hand, but I do think, regardless of how you do it, I would recommend to have it be presented or voted on whenever you want, but I

think earlier is better for us than later. That's just my own personal opinion.

MR. BEALES: Well, the other approach that occurs to me we might take, a little bit like Lance's, and I think speaks to the timeliness of it, the part of it that's concerning and that I'm not sure I feel I know enough about is how is the internal information sharing working now and how would these recommendations sit on top of that approach, and how would they affect that approach, and I'm not sure we know the whole story here.

A way we could approach this is to narrow these recommendations now to the interagency sharing and go back to the Subcommittee on what should we be doing, what should be different about the intra-agency sharing. And I'd be interested in David's reaction to that too, since I'm sending this back to you.

MS. MCNABB: Maybe including hearing a little more from Martha on the intra sharing.

MR. BEALES: Yes, at the Subcommittee level or perhaps at the next -- probably at the Subcommittee level because we would want it to happen more quickly than that.

Ramon?

DR. BARQUIN: I just wanted to expand on both what you and Lance were saying, because my sense is that there is an urgency to provide a framework for the Department vis-à-vis information sharing and access with everyone else. I mean, that's here and now. And I don't think we would be doing anyone any favors if we put out a document that was going to be ignored because of the intra. Why not go ahead and do it, as you recommended, and Lance, to address only the inter and not the intra, because over the next few months this will start to inform the intra-sharing, and that's one that we should also then focus on maybe at the next one.

MR. DAVID HOFFMAN: I just had a question in response. When we had this discussion as a Subcommittee, one of the concerns that we had is if the reason for doing that is because the requirements of filling out SORNs and PIAs make it less relevant to sharing within the Department, I think it's then difficult to state for other agencies of the U.S. Federal Government that these obligations should apply to them when they don't apply within DHS.

So that was the reason why we thought it was

important, especially when sharing between individual components, to do two things. Number one, have it apply. But number two, to make sure that the individual controls that we were recommending were not bureaucratic or burdensome but were what we thought were the minimum necessary for responsible handling of data.

And so I think this discussion, I think we've been talking about the process of the discussion, but I don't think we've gotten to the second point, which is do we really think any of these controls are burdensome? I can understand that maybe having to execute a formal agreement between one DHS component and another DHS component might be burdensome, and therefore I'm prepared to make a recommendation to take that recommendation out and to include language that would state that in those sharing situations between two components would be then less formal but still the creation of a document that makes clear how the information needs to be handled.

But I'm very sensitive to putting a recommendation out there saying that there are two different kinds of sharing situations, one where you share with other Federal Government agencies and one where you

share with other components within DHS, and we're not putting any of the obligations on the sharing within DHS. That doesn't necessarily make sense to me.

MR. BEALES: Annie?

DR. ANTON: So as a follow-up to David's comment, in my Subcommittee, where we were looking at the actual template, we had several interviews with the folks who actually work with the templates, and I know Tom and Renard were in these meetings, so they can correct me if I'm wrong. But the sense that we had was that they really didn't have that good of a handle on what information was actually flowing and what agreements were in place inside and outside, and that concerned us.

So our attempt, I believe, was to actually make recommendations that would help DHS, and also in terms of their practices in terms of the way that they set up agreements, and in terms of these guidelines. So I concur with David that we want the report to be taken as useful, and we don't want to make recommendations that may undermine your efforts or be seen as especially burdensome. And yet I think we need to find a sweet spot of what kinds of guidance we could provide that might encourage a little

more governance and transparency to prevent things that might pop up in the future, unexpected things. And I think having some kind of structure in place that we do the same thing that we ask others to do is a good idea. So I'd just like to leave it at that.

MR. BEALES: Neville?

MR. PATTINSON: Just to add, and I'm probably speaking a little bit out of turn, but on the service-oriented architecture activities that we are looking at, there is a definite need to simplify the world in how one goes about looking at the complexity of a system. We're already looking at an SOA environment which is very complex, built from existing implementations of various stovepipe applications now having to learn to interact with each other through service-oriented architecture mechanisms.

One of the key things that I saw there was the fact that we need to define the boundary of where we're working. And to me, the internal part of this between all of those stovepipe systems that are now trying to interconnect, that's an internal problem to DHS, and that's why we have PIAs for each of those systems. And with the

direction of that Subcommittee, we will now look at what we can recommend to look at that information sharing and how those relationships work.

What I clearly need is to kind of draw the boundary around the internal versus the external. To me, it's about your interfaces to where you're out of control from an internal influence. So that, to me, is very much the case of you need to have very strict practices and procedures around instances where it goes outside of the one DHS, so to speak. So those are the important areas to me to focus on first, that you have your interfaces to the outside world well controlled. The inside area I think is something that can be looked at through the work in the SOA, through perhaps some more work on the internal side. But right now, it's define your interface and make sure the gaps are plugged where you've got your leakage to the outside world.

So I certainly would echo the thoughts of what you're recommending, Howard, to define it to the external today and then look at, through SOA and through other activities, what are appropriate mechanisms, through PIAs, through whatever it is, to join these things together in a

way that they are consistent and controlled.

MR. BEALES: John Sabo?

MR. SABO: I mean, as a Committee, we've been working with DHS and components for many years now and we understand their commitment to privacy and bringing some structure to privacy, governance, and policies, and assessment and management, and we don't have the same confidence about external participants in the data sharing at all. And I've been arguing, as you know, for years that we need greater attention to policy rules and technical controls, and we don't have that. And partly we don't have it because we haven't had anything like this before. This is a perfect start, but it's still fairly high level and abstract. It does not define specific controls. It asks a set of questions and sets some boundaries.

So I guess, to be helpful, it seems to me, I guess I'm agreeing with Neville in the sense that we know what DHS is doing. We have opportunities to continue to work to influence that. We could take time to assess where they are internally. But on the outside boundaries we have no knowledge of what the external users are doing and the controls that they need to follow.

I think this would be a great start, a stake in the ground and lay this out for any external sharing, and it's not just -- it's with other agencies. It's with external organizations. I presume it would apply to contractors who are participating with DHS.

So I guess my sense is to move it forward, make very clear this is Installment A of the white paper and that it's laying out an initial set of guidance and recommendations on external sharing, but the Committee will move very quickly to assess internal practices and governance policies and technical arrangements. So that's my two cents worth.

MR. BEALES: Kirk?

MR. HERATH: I think what you read here is that philosophically I think a lot of us have some issue with the one DHS policy. I mean, it's --

MS. CALLAHAN: Well, we can't change that today, Kirk.

MR. HERATH: It's not hidden. No, and I don't think that -- and this isn't going to be law or anything. This is what we think is a best practice that should be considered, and I do believe that any interface, there

should be some fairly -- a good record. Just because you have the right to share does not mean you have the need to share. Someone should be thinking about these connections. So I'd like to keep it like it is.

MR. BEALES: Annie?

DR. ANTON: I wanted to add a note that I agree that external is clearly important. There's always the concern about whether or not we actually have any control over that, but it's important to have agreement. Not being a lawyer, I still understand having the agreement actually helps, right? At least you have something to go back to.

And in terms of the internal, I did want to note that DHS has come a really long way and that everyone that we've spoken with, they really are actively seeking ways to improve data governance and improve the way that they are collecting and sharing information, and everybody is certainly very concerned about doing it the right way. And so I think the recommendations we made were in that spirit of trying to encourage more of that. So I just wanted to add that. Thank you.

MR. BEALES: Are there other -- David.

MR. DAVID HOFFMAN: I have a recommendation.

MR. BEALES: All right.

MR. DAVID HOFFMAN: My recommendation is that the first edit that I described state that this document only applies for sharing between DHS and with organizations external to DHS, and then that the Committee recommends that DHS review these recommendations to determine which would be helpful in situations with sharing within DHS. And then that would -- I would take back the edit on page eight and go back to the original text.

DR. ANTON: Is that a motion?

MR. DAVID HOFFMAN: It's a recommendation for discussion first to see if people object, and then I'll leave it to the Chair to make the motion.

MR. BEALES: Was there a -- did you want to comment on that, Annie? I'm sorry -- Dan.

MR. CAPRIO: Just a quick question, Howard.

Thank you, David, for your Solomonic wisdom here. But can you repeat the language so that we're all -- I mean, this is very important -- so that we're all on the same page and that we have an exact idea of what we have on the table?

MR. DAVID HOFFMAN: If someone else can talk

for about a minute while I write it down, then I can.

MR. BEALES: Well, I can try what I think you said, and you can tell me if I did it wrong, that --

MS. CALLAHAN: Howard, I know you can talk for a minute.

[Laughter.]

MR. BEALES: It's true.

In that first edit on page one, what would be added to the printed text is at the end of that second sentence for sharing so it reads, "Personal data is respected and protected for sharing between DHS and organizations external to DHS. The Committee recommends that DHS review these recommendations to determine which are helpful," and then I think I degenerated a little, but "in internal sharing practices."

PARTICIPANT: Howard, I'm sorry. Could you do that one more time? I didn't get all that. Can you specifically say where you're starting and slowly read it?

MR. DAVID HOFFMAN: Howard, I'm ready now.

MR. BEALES: You are obviously better at this than I am.

MR. DAVID HOFFMAN: I am starting in the last

paragraph of page one, inserting a section in the sentence before the sentence that starts with “Governments have recognized there are two key elements.”

So the previous sentence that starts with, “It is critical” would remain as is. And so it would state, “It is critical that DHS establish specific policies and practices to govern broad information sharing to ensure that personal data is respected and protected for sharing between DHS and organizations external to DHS. The Committee also recommends DHS review the recommendations in this paper to determine which may be appropriate to apply to information sharing within DHS.”

MR. BEALES: If we do that, David, on that approach, it seems to me we also need to change the first recommendation on page two, which now says, “The Secretary will direct all components to utilize ISAAs when sharing personal information within DHS.”

MR. DAVID HOFFMAN: That’s correct.

MR. BEALES: And those three words should go on that approach.

MR. DAVID HOFFMAN: Correct. That’s a good catch. So deleting on page two in section one “oversight” in

the second line, deleting “within DHS and.”

MS. MCNABB: Howard?

MR. BEALES: Yes, ma’am.

MS. MCNABB: Dan’s tent is up, too.

MR. BEALES: Joanne, go ahead.

MS. MCNABB: Okay. I have a suggestion, David, for your -- I have a slight rewording suggestion in the sentence -- in the encouraging sentence. Let me just read you my suggestion. “The Committee encourages” -- I think that’s the way it started -- “DHS to review these recommendations to determine which may be appropriate to apply to” and I would say “information sharing among DHS components” rather than “within DHS.” That’s what we’re talking about. That’s what you mean by “within DHS,” isn’t it? Among components?

MR. DAVID HOFFMAN: I guess I was going for the super set to also say they’d want to take a look at if it’s sharing it within a particular component also. That’s why I phrased it the way I did.

MS. MCNABB: And so a component sharing with itself?

MR. DAVID HOFFMAN: Correct.

MS. MCNABB: Meaning sharing from one database to another?

MR. DAVID HOFFMAN: One program to another, potentially.

MS. MCNABB: Okay. I withdraw.

MR. BEALES: Are there other questions, comments, criticisms, arguments?

MR. DAVID HOFFMAN: Laudatory comments, notes of encouragement?

MR. SABO: I mean, not that it matters, but I think this is a tremendous start. So there, I said it a second time. You're not going to put in controls if you don't have a framework in which to establish the controls. So I think this is a great first start.

My comment was on number Roman II, Threshold Analysis. Does that need to change at all? "The Secretary shall require all components, CPOs and responsible parties lacking a CPO, to complete an information sharing analysis whenever they receive an inquiry for information sharing external to DHS"?

MR. DAVID HOFFMAN: Yes, Joe just mentioned it.

MR. SABO: Okay. Fine.

MR. DAVID HOFFMAN: It should say “receive an external inquiry for information sharing.” That’s another good catch.

MR. BEALES: If there are no further comments and those are just standing tents that haven’t fallen down yet, is there a motion to adopt the edited report or some other version of the report? Is there a motion?

Charles.

DR. PALMER: I’d like to move that we accept the document as most recently edited.

MR. BEALES: Is there a second?

DR. BARQUIN: I second.

MR. BEALES: All right. Is there any further discussion?

[No response.]

MR. BEALES: All right. Then all those in favor of accepting the edited document, please say aye.

[Chorus of ayes.]

MR. BEALES: All those opposed?

[No response.]

MR. BEALES: The report is adopted.

And again, thank you, David, and thank you,

everyone else on the Subcommittee, for your tremendous efforts in this regard, and we will convey this report in what will probably be my last official act.

MR. DAVID HOFFMAN: And I'd like to, once again, thank the members of the Subcommittee and thank everyone for this discussion, which I think was very helpful and makes it a better report.

MR. BEALES: We now come to the time for public comments, but no one signed up for public comments. So I guess at this point it is appropriate for us to adjourn.

Thank you all for being here. It's been a pleasure to see you, and I think we had an interesting and productive day. So, thank you.

[Whereupon, at 3:22 p.m., the meeting was adjourned.]