DATA PRIVACY AND INTEGRITY ADVISORY COMMITEE

PRIVACY OFFICE – DEPARTMENT OF HOMELAND SECURITY

PUBLIC MEETING

March 18, 2010

08:30 a.m.

The Tomich Center

111 Massachusetts Avenue, N.W.

Washington, D.C.

PARTICIPANTS

Chair:

RICHARD PURCELL

Participants:

LISA SOTTO	J. HOWARD BEALES
KIRK HERATH	NEVILLE PATTINSON
JOHN SABO	JOANNE MCNABB
LAWRENCE PONEMON	MARY ELLEN CALLAHAN
JAMES HARPER	REAR ADM. MICHAEL BROWN
RENARD FRANCOIS	TOBY LEVIN
ANA ANTON	MARTHA LANDESBERG
DAVID HOFFMAN	
CHARLES PALMER	
JOSEPH ALHADEFF	
LANCE HOFFMAN	
RAMON BARQUIN	
DANIEL CAPRIO	

Ms. Martha Landesberg: Everyone, we're about to get started, if you take your seats, members, and members of the audience. We're going to get started in one minute. So if you'd take a seat, that'd be great.

[background chatter]

Good morning, everyone. I'm Martha Landesberg, executive director of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. I welcome all of you to the March 18th public meeting, our first quarterly public meeting of 2010. And with that, I'll turn the meeting over to our Chairman, Richard Purcell. If I could just ask one thing, I apologize. Members, we don't have individual mikes for you this morning, but there are some mikes overhead. If you could just try not to talk over one another, that would be a big help to the court reporter. Thanks so much.

Mr. Richard Purcell: Good morning. Welcome to our meeting for the Data Privacy and Integrity Advisory Committee. I'm Richard Purcell. I would

like to ask if you would, please, out of a courtesy to all, to turn your mobile devices to a silent mode, so that they won't interrupt the scintillating discussion that you always do have. And we get distracted easily.

The other is that there are, as always, moments that we've reserved for public comments from approximately noon to 12:30. So if there are public comments that you'd like to make, to address the Committee, then please sign up at the table just outside of this room, please.

We're always – we always welcome those comments. And we'd like to have that dialogue. So please feel free to make them, but you do have to sign up outside of the room in order to do that.

We'd like to start today with our Chief Privacy Officer's update and welcoming Mary Ellen Callahan, the Chief Privacy Officer for the Department of Homeland Security.

[coughing]

Prior to joining – settle, wait for it, wait for it. Prior to joining the Department, Ms.

Callahan specialized in privacy, data security and consumer protection law as a partner at Hogan and Hartson, LLP in Washington, D.C. She's also served as co-chair of the Online Privacy Alliance, which was an industry self-regulatory group. She's also served as vice chair of the American Bar Association's Anti-trust Division Privacy and Information Security Direct Committee, sorry, that's right, Committee.

Mary Ellen has been the Chief Privacy Officer for the Department of Homeland Security for about a year now, right? This is an anniversary?

Ms. Mary Ellen Callahan: It is.

Mr. Purcell: Happy anniversary, Mary Ellen. We are delighted to welcome you here. We congratulate you on this first year. We've all been very, very happy to serve under your leadership. We welcome you to proceed.

Ms. Callahan: Thank you. Good morning, everyone. Thank you very much, Richard. And first, I want to welcome you to the Tomich Center here at the USCIS. As you know, the – as part of the

efficiency review, the Secretary has asked that all Committee meetings take place in a federal building if at all possible. And therefore, we have asked our colleagues at USCIS if we can also share the space with them. So I want to thank you. I think that this is a great space with great lights. And it's a little long. And I know that, but let's see how it works out. I think it's great.

As Richard mentioned, this is indeed almost exactly one year anniversary as the Chief Privacy Officer at DHS. And I think we had some really great results, great stories, and really, great initiatives in part thanks to you guys. So I want to thank you for that and also fill you in on what has been happening.

But first, I want to make sure that we all welcome a happy Sunshine Week. It is, of course, Sunshine Week in the Federal Government, recognizing the passage of the Freedom of Information Act. And we provided sunshine during Sunshine Week. So those of us who have been suffering through the Washington winter certainly appreciate the arrival of such a

week.

I'm going to provide an overview of several of the Privacy Office's activities since our last meeting in December. And as usual, there's been a lot going on in a lot of different areas. And I wanted to give you a picture of what my staff's been working on and what's been going on.

After that, Admiral Michael Brown, the Deputy Assistant Secretary for Cybersecurity and Communications, a DAS in the National Protection and Programs Directorate, will provide an overview of computer and network security and privacy protections in the Department.

After that, we have a bittersweet presentation, where we'll hear from Toby Levin, Senior Adviser and Director of Policy and Education in my office. And we'll discuss our work on several privacy related federal interagency initiatives.

Toby has been phenomenal in leading the privacy conversation at an interagency level, and really has been an exemplar, and a privacy advocate in the best sense of the word.

As you know, this is going to be Toby's last chance to address the Committee as a member of my office. Toby is retiring after an illustrious 25 years in federal service. And during her five years at the Privacy Office, she has worked tirelessly to further our message of systematizing privacy throughout DHS. And I want to thank Toby. And as I said, we will definitely miss her in the office. And I know the privacy community here in the Federal Government will as well.

In the final portion of today's session, the Committee is going to be discussing two important draft reports. First, proposed recommendations of the Department's use of enterprise service buses prepared by the Data Integrity and Information Protection Subcommittee and then proposed recommendations on Department privacy regress programs prepared jointly by the Privacy Architecture Subcommittee and the Data Acquisition and Use Subcommittee.

And I want to thank the – all the Subcommittee members for their diligence. And I

look forward to hearing your discussion later on this morning. And I think it's great to see that we have basically reports from every member of the Committee that are going to be discussed here publicly today. So thank you for that.

So what have I done for the past year? There has been a lot going on in my Office over the past year. And it's been really phenomenal.

One way to talk about what I've done is to talk about quantification, numbers, measurements. So during my tenure at DHS, we have done 518 privacy threshold analyses – assessments, 68 privacy impact assessments, and 62 system - system of records notices.

And that, of course, is the cornerstone for our compliance requirements. But in addition, on initiatives that have been started over the last year, the Department – the Privacy Office has reviewed 436 I&A analytical products since the Privacy Office and the Office of Civil Rights and Civil Liberties began reviewing our office of Intelligence and Analysis products that are

distributed to, for example, Fusion Centers and to other states and local partners.

We have had – which I'll talk a little bit more about - reviewed 10 Fusion Center privacy policies, have approved 10 Fusion Center privacy policies, a new initiative for reviewing the privacy policies to make sure that they are at least as comprehensive as the federal baseline capabilities document. And I have six more in my office right now. And as I said, I'll talk a little more about that.

I personally have participated in 12 advocacy or outreach events, totaling hundreds of different advocates or the same advocates 12 times. At the same time, as you know, that's an important part of my mission and of my tenure.

The – and I've started – I've given 25 speeches, about half of those in government settings and about half of those in public settings.

Again, trying to provide a message for the Department, message for the Privacy Office, and the importance of operationalizing privacy and having it

be part of the dialogue when developing programs and technologies.

And so, the other thing that they got, I counted it out, we have worked with at least – we've worked with every component at least twice on initiatives, including having people - Privacy Officers required in each of the components that deal with personally identifiable information and actually the FEMA Privacy Officer Tom McQuillan is here today. And I wanted to welcome him. And we have several other Privacy Officers, but they're old hat. So I'm not going to recognize them.

But it's been great. It's been wonderful to have this an opportunity and to work on maturing the Privacy Office and privacy protections within the Department.

We, of course, have been working on transparency issues and on disclosure issues, both in terms of on the FOIA side and on the privacy side. And I'll talk a little bit more about that in a minute.

I wanted to start today's overview, first, though, to talk about the international front. We've been extraordinarily busy on that. And in fact, I've just returned from intensive engagements with our European partners in Brussels, Strasburg, Amsterdam, the Hague, and Berlin. Five cities in four days. And this was in part as a follow-up to Secretary Napolitano's recent meeting in Spain with the German Justice Minister and also related to an increased dialogue and increased, as I said, transparency and awareness on an international front.

As with many of my outreach opportunities, I talked about the office, explained it, which obviously, the federal -- U.S. federal system for privacy is different than the European system - and talked about those differences, tried to dispel a lot of myths that exist both in terms of U.S. privacy issues on the federal side, as well as on the private sector side. I was a little bit of an outside counsel going back to my old days, but to also talk about kind of the institution and to build

in support for the privacy protections that the Department provides.

We also talked about the Department's use of Passenger Name Records. And our -- the report that my office did associated with the joint review of the U.S. EU PNR Agreement for 2007. And I'll talk about that during the compliance period.

Several other international events that have been going on, DHS, State and the Justice Department recently hosted an Austrian delegation to discuss the Preventing and Combating Serious Crimes Agreements, required for each country -- individual member state country to sign in order to be part of the Visa Waiver Program. So we talked again about privacy questions that they have.

We -- and then as I mentioned in February, in between two of the biggest snowstorms that Washington has ever seen, on the 8th and 9th of February, we -- my office hosted a delegation, together with Customs and Border Protection and the -- both the Office of Field Operations, the CBP Privacy Office, as well as the Office of

Intelligence and Operations Coordination.

The delegation from the European Commission and from European member states for a joint review of the DHS privacy practices under the 2007 EU U.S. PNR Agreement.

In preparation for that review, our compliance group updated its 2008 report concerning Passenger Name Records derived from flights between the U.S. and EU. That report is available outside and I believe is in your packets that you received earlier.

The updated report that we did in February finds that CBP has taken action to address all the six outstanding recommendations that were contained in the 2008 report. And in addition, we found that CBP continues to comply with the terms of the 2007 U.S. EU PNR Agreement.

We then issued a joint statement together with the Commission and with the member states to say that indeed this joint review took place. It's the first joint review under the 2007 agreement. We -- the review itself included site visits to the

National Targeting Center and the PAU at Dulles Airport, as well as comprehensive briefings from Customs and Border Protection and from the Privacy Office about what terms are supposed to be, you know, about the -- in terms of the review. And I think it went quite well personally. I think it was a very collaborative conversation. I want to thank the over two dozen DHS employees who were able to get in on Monday and Tuesday, February 8th and 9th, to help participate in these dialogues and these discussions.

And there will be a report issued by the Commission probably next month associated with their conclusions from the review. And we look forward to seeing that report.

In early March, my deputy, John Kropf, travelled to Strasburg, France to participate on behalf of DHS as an official observer in the Counsel of Europe Consultative Committee on the Convention for the Protection of Individuals with Regard to the Automated Processing of Personal Data. So that would be convention 108.

It's great this -- the event marks the first time the Federal Government, the U.S. Federal Government has participated. And the Federal Government was granted observer status late in February, and then was able to attend. And again, it's another place to have a dialogue about best practices and international privacy standards.

I anticipate the Department of Justice will join us. They also, as I said, the government was granted status, given that there are several Ministries of Justice, administrative computer privacy officials, it's a natural ally to have Justice (coughing) in this observer status.

Another major initiative, obviously, of my office is to -- is information sharing and making sure that information sharing is systematized and considers privacy protections throughout the Department. As part of that initiative, I'm pleased to announce that in December, Helen Foster joined our office as a Senior Privacy Analyst. Helen has been focusing on building privacy protections in information sharing arrangements within DHS, as well

as with external partners. Helen has a long history working as a private sector lawyer, but also at the Federal Trade Commission and really brings a great background to help us with these issues.

She's actively been engaged in revamping the DHS information sharing guidance, including major revisions to data information sharing access agreement templates, guide book, and data access request processes. And these draft documents are currently being vetted within DHS. Furthermore, she -- the documents - her edits expressly incorporate the recommendations and concerns from the Committee in the May 2009 White Paper on DHS Information Sharing Access Agreements. And Helen will report more fully on that during our next meeting. I'll ask her to give an update to the Committee on those issues.

In addition, Helen has been providing privacy expertise and support to a White House initiative to develop a national strategy for secure online transactions, which focuses on strategies to implement identity management solutions to enhance

the privacy and security of online transactions across the government and private sector.

And that, too, I hope to have more -- I hope we can have a discussion on that more fully in May. And I'm excited about her being a part of the office. And I want to thank her for her leadership on these issues. You know, I said, okay, go do it. And she had to provide a great deal of support to Ken Hunt, who had been working on information sharing within the Department within the interagency opportunity, as well as with Fusion Centers. And so now Ken is focusing together with Lynn Parker, my special assistant and others on Fusion Center initiatives, which is another major push for us in 2010.

As you are aware, we launched one major initiative in Fusion Centers late last year, which was to have the DHS Privacy Office as a co-chair of the Information Sharing Environment's Privacy Guidelines Committee to review the -- each of the privacy policies for the Fusion Centers, particularly those who -- so there are 72 Fusion

Centers that are recognized, so to speak. And for those 72, those are the Fusion Center privacy policies that we will be reviewing.

In addition, in December, I was not yet able to announce this, but in the Department as part of their 2010 grant guidance, specifically required that any Fusion Center that got DHS grants had to finalize their privacy policy and have it approved by my office within six months of their -- of receiving the 2010 FY 2010 money. Otherwise, they would no longer be able to receive money but for finalizing the privacy policy.

So that has received some attention. It's great because as U.S. privacy professionals know, sometimes privacy only has a carrot. It can only induce people to do things. Come on, (coughing) it's a good thing to do. In this circumstance, we have a carrot to go and say this is a good thing to do. It's good for fusion centers, but also we have a stick. And I want to thank the grant guidance staff in DHS for allowing us to do this and have this -- these synergies. But it's also the right thing to

do. This is -- it's important for Fusion Centers to recognize privacy protections and to incorporate them. And for that reason, we're really having a big push on having these privacy policies be sufficient and mature, and to refine them going forward. And we have had success with that. And we're very pleased for that.

Together with that, as another part of an initiative, working with our Office of Civil Rights and Civil Liberties, who of course, is our sister or sibling agency here at DHS. We are working to provide more privacy and civil liberties training expressly to Fusion Centers. The Office of Civil Rights and Civil Liberties has an extensive privacy and civil liberties training program that they provide to Fusion Centers upon request. But of course, that's not scalable. And so this year, we're taking our next initiative, which was the next requirement that we had towards Fusion Centers, and going to train the people in Fusion Centers to provide privacy and civil liberties training. And so, it's a train the trainer session that will take

place in the four regional fusion centers conferences. And we've received the support of the Information Sharing Environment Program Manager to help have all the privacy officials coming in to participate in that training. And I think that, again, is another way of maturing privacy issues within the Fusion Centers and to understand them.

At the end of February, I and a number of my staff attended the National Fusion Center Conference in New Orleans. And this is an annual tradition. And I, as part of this tradition, we had a lot of outreach. We had a learning lab related to privacy and civil liberties protections. And again, because of the privacy policies, we got some renewed interest.

And furthermore, I participated in a panel on Privacy and Civil Liberties 101, together with the Office of Civil Rights and Civil Liberties, as well as my colleague, the Privacy and Civil Liberties Officer at the Department of Justice and the FBI Privacy Officer. And that was great.

In addition, I addressed a private meeting of Fusion Centers across the country on the

developments that I had just briefed you on. And I thought it went quite well.

As I mentioned at the beginning of my presentation, we have approved 10 privacy policies. And we have six more in my office. And we understand that there are several more that are soon to come forward.

In terms of timing just so you guys know, the grant money will probably be distributed in early summer. So we're talking June, maybe early July at the earliest. So a six month clock from there puts us basically as a calendar year review process. And our team is prepared and ready to be able to work on those issues. So we're quite pleased with that.

Later on, there's going to be a significant discussion on cybersecurity. And we will have Admiral Brown here to discuss this in more detail. But as part of my report to you, I wanted to just go over – briefly mention a few of the Privacy Office's cyber activities.

The – as you know, the White House recently issued an unclassified description of the

comprehensive National Cybersecurity Initiative and published it on whitehouse.gov. This is consistent with more openness and transparency. We, as part of the DHS Privacy Office, had -- we have published a PIA on a proof of concept pilot on Einstein 1 capabilities with the U.S., the Department and the State of Michigan. There is a copy of that in your folder. So the PIA. That is, of course, publicly available. And it's also available on the table outside.

As a more overarching approach, together with the Office of Cybersecurity and Communications, Admiral Brown's Office, my office published a white paper on the Department's activities in the area of computer network security and privacy protection. And there's a copy of that, again, in your folders, and again available publicly. That, too, is available on the DHS website, particularly in a new section for cybersecurity and privacy protections. All of those documents I've discussed are posted there. And I think that's a good way of talking about the scope of cybersecurity issues, and the role of my office

for integrating privacy protections into them.

The Compliance group is consistently busy. I stated the numbers for the PTA's and the PIA's. And they, of course, are the bread and butter for privacy compliance within the Department. To help them better manage the compliance documents and to ensure that the group's output is organized and timely, I've assigned them a near full time administrative assistant, who will take the lead in tracking compliance documents through our new compliance tracking system, for which we have a PIA.

So we have that in – we have that. And in effect, Erin(coughing) you know, supports DPIAC. Erin will be migrating some responsibilities to support compliance on more of a full time basis.

Another one of my initiatives for last year that some of you know about is the development of an updated PIA. The Compliance group is nearing final development of an updated PIA template and guidance document. Since the Committee's last meeting, the group has distributed drafts to the Privacy Office

Directors, Component Privacy Officers, Privacy Points of Contacts, and the Office of General Counsel for review and comment. We will release it, not we plan to release, we will release the new template by our annual privacy compliance workshop on June 10th. And I'm – I very much think that this will help provide more transparency, but also privacy analysis within the PIA in a more streamlined fashion.

Other things the Compliance group is working on together with others in our office include working on improving the Section 803 report in response in part to your feedback associated with the quarterly reporting on complaints and incidents that we have to make to Congress.

Specifically, we've enhanced the transparency for the first quarter report by adding narrative examples of the types of review we've conducted, the types of complaints we received, and how we resolve them, and by clarifying the categories of complaints and their disposition. Again, a copy of that is provided in your folder and is available on the desk

outside.

We have issued revised reporting guidance to components consistent with these changes, of course, and plan to implement additional improvements, such as providing more context for the training data we receive.

And I'm quite pleased about that. And again, I think it will help all of us explain the Privacy Office.

Furthermore, as you know, my office has been – it's mainly involved in the Department's planning for use of social media tools and initiatives. In addition to providing policy support and development, the Compliance group has drafted a social media PTA, two social media PIA's covering social media and network interactions, and informational push - not interactive - media. So those are going to be the two types. We're going to have interactivity, and then the non – basically the non interactive social media, where we provide the information, together with our Office of General Counsel, our Chief Information Security Officer,

and our Public Affairs Office. We're in the process of developing a social media compliance process for the entire Department in terms of utilizing social media tools for providing the Department's mission.

We're also at the final stages of developing a process for computer matching agreements and establishing a formal Data Integrity Board. And we will be doing that very soon. The Compliance group has drafted a management directive. And we'll be finalizing the CMA template, as well as training for the Data Integrity Board members.

We have been supporting the CIO Council's Identity, Credentialing, and Access Management Subcommittee by drafting a model PIA for federal agencies considering the use of commercial credentials, such as Google and Yahoo to register individuals at federal websites. And you'll hear more about the CIO Council work and more of the interagency work from Toby Levin when she speaks later on today.

In January, Rose Bird and I briefed the House Homeland Security Committee on the privacy incident

management work, including the complaints tracking system, as well as the Privacy Office's role in DHS TRIP.

Then we have the Privacy Incidents and Inquiry Group has also undertaken two initiatives in response to inquiries from this board, from this Committee. In February, we queried the Component Privacy Officers and Privacy Points of Contact to obtain information on component privacy complaint handling processes and procedures, the tools to manage those complaints, and the availability of complaint handling metrics. And that process will enable us to identify best practices and to assess the feasibility of any additional data, not just to our 803 reports, but also to our complaint tracking system and processes within the Department, and within the Privacy Office.

And second, we hosted the second DHS Privacy Incident Handling Quarterly meeting in February and presented an overview of incidents within DHS for the third quarter.

I mentioned it's Sunshine Week. That,

obviously, is an important element of our office, our Freedom of Information Office, which is the, as you know, the office has two sides. And I'm pleased to announce that our FOIA team continues to grow. And we have in the past several months added six new FOIA specialists. And a new administrative specialist will be on board soon. And that will certainly help us manage the FOIA flow, which has increased in the administration in light of the several openness and transparency initiatives that the president has implemented.

Last month, we published the fiscal year 2009 FOIA report to the Attorney General. That's the process - we publish it to the Attorney General. And that – and then in addition, we published a first ever Chief FOIA Officer's Report on Monday. And that is a new initiative. Again it is required by the Attorney General, who has been asked to report the fiscal year report basically says numbers. What have you done, how have you done them, and how are you doing in terms of your backlog?

And the Chief FOIA Officer's report is more

focused on the open environment and transparency initiatives and what we have to do associated with the open government initiative and also in terms of addressing the backlog.

And as the Committee is very aware, DHS when we began operations, it inherited a huge backlog of FOIA requests from its legacy agencies. And furthermore, then the creation of DHS itself generated a flood of new requests.

The result was a backlog of 98,396 requests at the end of FY 2006, which was the largest FOIA backlog in federal history. Woo-hoo, we're number one.

[laughter]

But as a result of the dedication of the DHS FOIA Professionals, and through sheer, you know, manpower and legwork, the Department has reduced its backlog by over 80 percent in the last three years. Plus, as of January 2010, the DHS backlog was down to 12,000 requests, which is really a Herculean effort on their part. And I wanted to thank them for their hard work related to that.

In addition, we are also taking a very aggressive approach to proactively disclosing information in keeping with the open government directive and related transparency initiatives. We believe that this will have an effect to further reduce the number of FOIA requests because the information that's being sought has already been made public.

The Department has made significant enhancements to its online FOIA reading rooms, as well as having new information posted. We've disclosed over 600 documents on a proactive basis, including management directives and other opportunities totaling close to hundreds of thousands of pages proactively disclosed. And furthermore, we will be doing more in the future. So I think it's been a great initiative in terms of disclosing these types of things in a proactive way. And for that, consistent with the Administration and consistent with our obligations as professionals to engage in transparency and openness, whether it be on privacy side or on the FOIA side.

With that, Mr. Chairman, that concludes my report on the activities of the Privacy Office since we last met. And I turn it back to you.

Mr. Purcell: Thank you, thank you very much. You may ask a question, but I'm going to use the Chair's prerogative and ask mine first.

[laughter]

I note with interest, Mary Ellen, the model PIA for use of commercial credentials. Can you explain a little more about that? I think that the Committee has a keen interest in perhaps some ability to help with that process.

Ms. Callahan: I actually think Toby's going to talk about that during her session.

Mr. Purcell: Oh, is that right?

Ms. Callahan: Yes.

Mr. Purcell: Okay.

Ms. Callahan: So I think she can go into it in a little more detail about that. She has been working together with compliance group about several different identify management – making sure that privacy protections are included in that. So I

think she may do that —

Mr. Purcell: Yeah.

Ms. Callahan: -- or better suited to do so.

Mr. Purcell: Fine. We'll look forward to that from Toby. Joan, do you have a question?

Ms. Joanne Ms. McNabb: I was interested to hear you talk about the new requirement for grant applicants relating to privacy policies. As you may recall from the meeting we had when you were an observer before your official unveiling, we had put forward a request that the grant application process include gathering information on whether PII is going to be collected as part of whatever is being proposed, and have run into various procedural hurdles for a number of years on that point.

Ms. Callahan: Yeah.

Ms. McNabb: And so, my question is with what you were able to do by some miraculous way, will that reveal – will the fact that they have to provide a privacy policy, will that in any way reveal whether the project collects PII?

Ms. Callahan: That is a great question, Joan.

And the provision of federal grants to state and local organizations, as you know, is a multi layered and complicated process. And I am by no way an expert in this issue.

The requirement to provide this type of information and together collect – and to ask about are you collecting PII, where are you collecting PII? As I understand it, that is outside – it is outside of our purview to do that kind of discrete specific element.

What we did do for the grant guidance is, as I said, for this required, you have to have a privacy policy that's at least as comprehensive as the baseline capabilities document. It doesn't have to be a mirror, because obviously, state law, you know, obviously California has unique state laws and so on, but it has to at least have the same fundamental privacy principles within it. So that we thought we could do and have a requirement in that way.

Something else that we were able to get into the grant guidance this past year was related to closed circuit television, which is also an issue of

– that has been before this Committee. We have required – we have urged and encouraged, those are the words that we could use, urged and encouraged that those individuals who are either launching a new CCTV program using DHS funds, or having a continuing program, to do PIA's. And we pointed them to the Department's closed caption television PIA for state opportunities.

We've had several questions about that. I'm working with the grant guidance staff to try to get a little more robust disclosures.

Ms. McNabb: Can you urge and whatever that other word was you said, encourage them to reveal whether or not they're going to elect PII along with your urging and proposing?

Ms. Callahan: If – well, yeah, so in the PIA – –

Ms. McNabb: In the spirit of our official requests.

Ms. Callahan: Yes. So the – as I said, the requirements on a federal level from a Department perspective is difficult to put too many kinds of

prescriptive requirements on it. But I have tried to work with the grant team to not only have these two elements, but to have privacy protections considered in the grant guidance process. That I hope to have for the 2011 guidance, which is coming up. So—

Ms. McNabb: Okay.

Ms. Callahan: Right. So on the PIA question, I don't think I can ask expressly.

Ms. McNabb: But can you urge and encourage?

Ms. Callahan: I think I probably can urge and encourage. And as I said, it's part of the PIA process –

Ms. McNabb: Will you?

Ms. Callahan: -- for – I think if I can I will.

Ms. McNabb: Yeah.

Ms. Callahan: I mean, I don't know if I can. But I'm still trying to figure out that legal hurdle because that is a very unique legal skill, federal grant provision.

Ms. McNabb: Yeah.

Ms. Callahan: Yeah. So but as I said in the CCTV PIA, they would have to disclose that as part of the PIA anyways.

Ms. McNabb: Uh-huh. Thanks.

Mr. Purcell: I'm advised that our next guest is on a tight schedule. So I would like to ask the Committee to be very brief in their comments if we can, please. And in – and also, Mary Ellen, you'll be with us for –

Ms. Callahan: All day.

Mr. Purcell: -- for the morning. So those members who can hold in abeyance their question and bring it up at a later moment in this morning, you'd be welcome as well for that. So if there are people who are – continue, no?

Ms. Callahan: Encourage them.

Mr. Purcell: We can leave them? All right, fine. I've changed them into –

Mr. Joseph Alhadeff: No, I think you encouraged –

[laughter]

Mr. Purcell: I encouraged the -- which is in

my program. Thank you, Mary Ellen, very much --

Ms. Callahan: Sure.

Mr. Purcell: -- for your presentation. We appreciate it. And yes, and we will, I think, take up a little bit of time as the schedule allows to further our discussion –

Ms. Callahan: Absolutely.

Mr. Purcell: -- this morning.

This morning, as well, we're privileged to have with us Rear Admiral Michael Brown. Admiral Brown is the Deputy Assistant Secretary for Cybersecurity and Communications in the Department of Homeland Security's National Protection and Programs Directorate.

Admiral Brown has – he plays a leading role in developing the strategic direction for the cybersecurity and communications components. This includes the National Cybersecurity Division, the Office of Emergency Communications, National Communications System, and also serves as the Assistant Deputy Director of the Director of National Intelligence's Joint Interagency Task Force

for which there is an acronym, but it's actually longer than saying the words.

[laughter]

Admiral Brown has served in the Navy for 28 years. Prior to his assignment as the Deputy Assistant Secretary. He served as the Director of Information Operations Divisions and Deputy Director of the Cryptology Division on the staff of the Chief of Naval Operations.

In both those roles, he led the Navy in expanding its operational role in cybersecurity, cyberspace, and other technology implementations.

So Admiral Brown, welcome. We are delighted to have you with this morning.

Rear Admiral Michael Brown: Thank you very much, Mr. Chairman. It's actually up to 30 years in two months.

[laughter]

When we wrote that bio when I first got to DHS, my aides tried to say almost 30 in the – and it was going out. And I didn't want to appear older than I was.

[laughter]

I can no longer hide. So thank you very much for the opportunity. I do have a few slides. And I know that the briefs were available.

I really just want to use a couple of the slides to talk about the current status, what we've been doing. But as I just saw, and as I know many of you, I would like to engage in a conversation. So I urge and encourage you to ask questions when we go to that.

We'll start with the threat, which is slide three. It's something that you are all very aware of. It's something that we see every day in news media. It's something that we in our business, in all of our public private sector partners are dealing with on a daily basis, the fact that the threat is more targeted. Obviously, it is louder, more pronounced. We're seeing that. And they are becoming more sophisticated.

So what I'd like to do from now on is talk to you of what we have done and what we were continuing to do, what DHS is doing, how we fit into the

national effort and how we are working with the private sector also.

So as background, many of you are aware that the President Bush in January of 2008 solidified the comprehensive National Cybersecurity Initiative through the NSPD 54 HSPD 23. And that was just a couple of weeks ago released or summarized at an unclassified level by the White House while we were out at the RSA conference.

So for the first time, a large majority of what the CNCI was about and the NSPD, that we had to release to the unclassified level. And DHS has a number of roles to play. We have a leadership role. And we have a specific text for the initiative. And I encourage you to ask questions, should you desire to find out what specific goals are.

The next page lists the 12 initiatives. I won't go through them all, but I want to highlight several, where we are concentrating our efforts. In particular initiatives 1, 2, and 3, which deals with reducing the threat through a number of actions. First, by reducing the Internet access points and

coming up with comprehensive security standards that can be applied across the board. That is pretty much applied to initiative 1.

The second is to come up with intrusive protection capability and increased analytic capability through DHS responsibilities. That is where we have deployed EINSTEIN 2 and have increased our analytic and other capability in people inside US-CERT in the National Cybersecurity Initiative.

And Initiative 3 is something that we have recently started. And that has to do with not only understanding what the threat is, where they've gone, but start to prevent that malicious activity from taking place. That's the driver we call EINSTEIN 3. We are in the midst of an exercise and will be happy to take questions. And I'm here to tell you that the unclassified Privacy Impact Assessment associated with the exercise itself will be released either later today or by tomorrow. We are frantically finishing up that product to ensure that we have that unclassified PIA out there, so that people can understand that the unclassified

level, what we're doing with respect to intrusive prevention for the Federal Government, focusing on the civilian executive bridge.

A couple other things. Later on in those initiatives, like initiative 8, which is increasing the education for the federal workforce with respect to cybersecurity, we have a leadership role in that for the Department of Defense.

And two others. Lastly, Initiatives 11, working on supply chain, the whole idea with respect to the cyber – to the CNCI was the fact that there is no silver bullet to have a comprehensive, hence the title, approach to as many factors as could be addressed when looking at cybersecurity. So Initiative 11 is looking at supply chain and how we can help to address that piece.

And then, number 12 is focusing on public and private partnership. There are numerous things that we have done with respect to initiative 12 in the private sector to increase situational awareness, not just on the public sector side, but on the private sector side. And so, one of those things

little pilots that we have is the initiative where we have where we have EINSTEIN 1. And we obviously have a privacy impact assessment that's --.

Mr. Purcell: Okay.

Mr. Brown: Moving right along –

Ms. Callahan: It was my fault. Sorry about that.

Mr. Brown: See how easy it is to transition. That's because it's deep.

[laughter]

Frankly In fact, Mary Ellen, I wish I had been there for the unveiling.

[laughter]

Privacy actions that we've taken are, as we have said from the very beginning, extremely important to us and a foundational part of our approach inside DHS with respect to cybersecurity. So we work very closely with the Department of Justice as they went through the legal review as to what our responsibilities and capabilities are with respect to EINSTEIN 2. And that was released last year at the unclassified – it was an unclassified

effort.

With respect to our privacy impact assessments, you see three major ones there that we have had with respect to EINSTEIN 1, which is dealing with network flow, understanding what the traffic is doing, who it's going through, where is it coming from. And EINSTEIN 2, which has been focused on intrusion detection. So understanding what the (coughing) activity.

And as I just mentioned, we will shortly release the unclassified PIA for the exercise that we're currently undergoing, that will test the technologies we need to use for EINSTEIN 3. And we'll follow up on that.

And then, again, I think that a critical part of the teamwork is our engagement with you. So we've had several sessions. We will continue to have sessions where we can provide information and have discussions at the classified and unclassified level. I think that's critically important that we understand the world. And we're not going to completely understand the world. So we will focus

down and want to charge further engagement on Europe side as well as our side to make sure that we get there.

With respect to EINSTEIN 2, and literally for some of you who have been told to just – as we go to, not on the currently capabilities that we're using inside the exercise that as we get to EINSTEIN 3, we have developed numerous policies and procedures that frankly, I think are better than any place else inside the U.S. Government with respect to handling the information, to putting the policies and procedures in place, because we have, frankly, a lot of purpose, a lot of oversight, a lot of interest in what we're doing. And that's at the public sector side because I work inside the inner agency.

So for capabilities that are well known inside the public and private sector side, like EINSTEIN 2 as an intrusion detection capability, we have numerous detailed standard operating procedures and other policies that we put in place. And we do that in order to make sure that as we're attacking the

malicious activity that is out there, we are mindful of and have procedures to handle should we have any PII information and to ensure that our operators and analysts know how to handle the information.

We also -- you see that bullet up there on questionable activity. We also have procedures in place so that we could -- we know what to do should something happen, whether it's on purpose, and malicious in itself, or inadvertent. And so those were things that we've put in place.

And the last part is the fact in order to make sure that this was working, we've got auditing procedures in place to follow through on that.

If we could go to the next slide.

[laughter]

Get to some of the things that we've done with respect to implementation. Again, get into how we tried to go past the minimum requirements. We have responsibilities for memorandums of agreement with each of its departments and agencies. They certify that they have done specific things, including training and holding their operators, their users

accountable, as well as if there's a proper notification to all of the individuals that have access to the network and that they have policies and procedures in place. So that is part of the process that we go through. It's what I call the soft stuff leading the hard stuff. This individual handling, individual working with every department and agency by DHS in order to make sure that all of the partners understand what the roles and responsibilities are, and that they execute it.

The next slide is our oversight and compliance training. We established inside our office, inside my organization, an office that is – sorry, first I'll talk about Mary Ellen.

[laughter]

Ms. Callahan: Isn't that the order which it Should always to be in?

Mr. Brown: As I've already mentioned, and I've done this numerous times, the fact is that we came together and will continue to do so. And so, there are responsibilities that Mary Ellen executes for the Department that we follow to make sure inside

our organization, inside CS and C, we established oversight and compliance. So that and to the users, we are monitoring the post – or actually doing the mission, that we are setting up processes and procedures so that not only we are providing the appropriate oversight to the operators and the analysts, but there – we, my office, is capable of responding to Mary Ellen and her responsibilities, and to the Interagency, and for you all. So that is the structure that have been established inside DHS.

A couple of quick things now that I want us to talk about, that of how we're actually operating. We've established a National Cybersecurity and Communications Integration Center, where we have taken various aspects, various operational evidence of DHS, co-located it to be able to conduct operations in the environment and the – to be able to counter the direction that we see in physical and in cyber arena. So we are taking operational capability to focus on the communications and IT sector, co-located them and are now, for the last four or five months, begun to operate as a team.

And we're going to continue to expand that.

And part of it is when we brought the National Coordinating Center for Telecommunications onto the floor, we brought a private sector partner. And we're going to continue to do that. This gets to the next and my last slide, the next case we are feverishly working, which is the National Cyber Institute on Responsiveness. Called for underneath the – President Obama's cyberspace policy review. We've been leading the interagency and private sector effort to develop the incident response plan. And my premise from the beginning, my guidance to the folks that I've been working with is we never want to execute this. So when writing the plan, when aligning and assigning roles and responsibilities, we need to be practicing and operating the way we would execute the incident response plan. And so, that means steady state operations. So that is what we've done.

We've had several iterations of the document. I'm spending another three or four hours this afternoon in other sessions, working on this. We've

done table tops, interagency, and with private sector, a couple of private sector table tops to ensure that we can identify current capabilities and gaps, and barriers. So that we're capable of being better than we are today, which is better than we were last year.

And with that, I am at your service.

[laughter]

Mr. Purcell: Thank you, Admiral Brown. Are there questions for any Committee members? I'm going to start down here with John. Is that your (inaudible)?

Mr. John Sabo: Question on the broader mission, cybersecurity, you know, and the review of integrating, look ahead for some of the main clients even beyond that, new very sensitive infrastructures be respective of what happens in (inaudible) high drug action, we have security and privacy working for HHS to develop – to identify risks around privacy for health – electronic health records and integrated health records, critical in structure. Likewise, smart grid.

And we have (inaudible). I guess my question is from your perspective, being very concerned about the cyber CI aspect of the infrastructures, are you monitoring – do you have staff participating in monitoring that work? And being – do you see any potential projections to some small amount of research that might CI cybersecurity aspects of using health and infrastructure? In other words, it seems there are power electrics going on. The question is, are you able to pull that together (inaudible)?

Mr. Brown: Yes, so we have staff members and subject matter experts that are participating in – at various levels, all of the things that you mentioned. So first of all, looking at what the technical requirements are for cybersecurity with the health initiatives and with the smart grid. We are part of the working group that establishing the standards. And part of our process is – to not just look at the cybersecurity piece, but we have to address the privacy issues.

So part of what we've learned in the deployment

of EINSTEIN 2 is – as we build to EINSTEIN 3 is the, again, I get back to the soft stuff being the hard stuff, but the individual criteria for sharing of information in our mission space with respect to cybersecurity, that we have with the individual departments and agencies. So when I talk about they need to certify, part of that is how do we handle what is potentially sensitive information on their side?

Then you get into the private sector aspects that go along with that, which is the work that we do and try to bring to the table to the cross sector cybersecurity working group and the individual sectors, because that's our easiest and quickest way to get to the vast majority of the place to again address both of them.

Cloud computing, huge issue with respect to – it's got great opportunities. And if we are not from the beginning considering the cybersecurity aspects of it or – and part of what we're talking about is always probably the first, second, or third word is the privacy aspects. This is about

protecting privacy for our citizens. And be a part of the interagency working group that is working with the CIO's and the (inaudible) to ensure that we're trying to address up front cybersecurity as the Federal Government goes into the (inaudible).

Mr. Purcell: We will work around the table to my left. So if Joe, you're next up.

Mr. Alhadeff: Thank you. And it actually worked as a good segue, because my question really relates to the soft stuff is the hard stuff. You talked about having procedures for handling questionable identifiable information that was within the people that were part of EINSTEIN 2. Then you talked about rolling it out across the partners. And then you kind of spoke about the interface with the private sector.

So we seem to have perhaps four scope issues. We've got the people who are in the program itself, an intra DHS issue related to people who may be touching the program, external agencies, whether state or federal, who may become involved, like Michigan with EINSTEIN 1. And then finally, an

interface with the private sector.

And I was wondering, as those tools and processes get developed, and people start coming up with how we define certain terms, how we define sensitive and things of that nature, is there a harmonized process related to that? Or is that something that is done at every mission and every section, because as you get to the interface with the private sector, if everyone is using a different set of definitions and a different set of procedures, it's going to be very difficult to figure out how to manage those information flows, because people are talking about different things or same things in different ways?

Mr. Brown: Great question. So let me start with the soft stuff is harder than I actually talked about. And so, lexicon is a huge issue for us, even within the U.S. Government, what we're talking about. And part of that is because, obviously, being from the Department of Defense, what DOD says, the same words do not equate to the same mission space that we have inside DHS.

So it's very, very difficult to try to make sure that everybody understands that what we're saying. And so, we are trying to lay out the lexicon. It takes a long time when – and it is every step of the way a hard process. And in some cases part of what I've been saying since I've got the DHS is in many cases, it's the first time it's been done. So that makes it even more difficult to articulate what we mean, what the words are behind that. So that everybody is comfortable with the policies and procedures that we put in place.

Starting with the procedures that we've got for information handling and for PII, there – we put strict procedures in place so that if there's a requirement that you can tie malicious activity to specific PII as a requirement to capture that, it goes through a rigorous process.

The rest of the procedures are to prevent the PII from getting to all of the other partners that you've describe. There are specific technical things that we want to be able to share with our Federal Government partners. And there are

vulnerabilities and threats that we want to share with the private sector and want the seat coming back to us that we need to be able to share. But it is extremely complicated. It is time consuming. And we've proven that with our exercise. We've proven that with milestones that are taking longer, because I'll go back to every department and agency on the federal side has various levels of capability and capacity in, again, perhaps a different understanding of the words that are being used.

Mr. Purcell: Lance?

Mr. Lance Hoffman: Thank you. In your slides, you mentioned you were going to test some of the work you're doing during Cyber Storm III, coming up in September. Could you tell us just a little bit more about your planning of this, and in particular, of what you are doing with the Privacy Office in terms of both the planning and the actors during the exercise and the observers?

I ask this because I remember when I was first appointed to this Committee it seems like eons ago, there was a similar exercise we were invited to.

And when I got there, it was in the very early days of DHS. And there was some confusion. So I never got to see anything, what was going on.

And so, I'm hoping either for me or some of my colleagues, this will not happen again. And more importantly, what you're doing with the Privacy Office, integrated into the planning with that regards?

Mr. Brown: So as it says, this will be the third Cyber Storm exercise. It's done every two years. We are in the process right now of working along the individual elements that will be part of the exercise that we'll test.

It is being built, the scenarios and the objectives are being built with a combined private sector and public sector team. So that we can, in fact, test the incident response plan, because it's supposed to be natural in scope and be able to go against public, private sector.

In fact, some of the people in the private sector side that are participating in the scenarios and the objectives, have also been very big in the

development of --.

The timeline is I have to add – if the response plan done by the end of June, beginning of July, because we're going to have our final planning conference for Cyber Storm III at the end of July. So we've obviously got a better connection. So there's my drop dead date.

And then, we will formalize – I will work with Mary Ellen to make sure that we've got the invitations out. It will be held at a couple of locations where we don't obviously do the exercise over a live network. It is a disconnected enclave that we use for many reasons. And may be able to show some of the activity, I think at least at one of the locations. And it should be where the headquarters of the major portion of the exercise will be done. And we're working out to see if we can. And we'll be able to have the classified portion, if we needed to test classified elements, what we need to do on the public, private side.

Mr. Hoffman: But you will be involving as actors also the Privacy Office personnel?

Mr. Brown: What do you mean by actors? Do you mean as part of the scenario of development?

Mr. Hoffman: Yes. I'm not talking about --

Mr. Brown: So that happens – it definitely happens on the Federal Government side because if we're going to be a specific action, we're – with the policies and procedures, we need to test any of that -- Privacy Office is part of the review process.

So just like right now, I mean, we're – if we were to go down the path of a specific signature that was different from the template for (inaudible) capability and currently have privacy as part of it, as well as what you see. And we justify the exact reason why we're doing what we're doing. If it doesn't meet fair criteria, we start over.

Mr. Hoffman: Thank you.

Mr. Purcell: Ramon?

Mr. Ramon Mr. Barquin: Okay, if I can shift from the soft stuff being hard to the hard stuff being also really hard. I just wanted to get a sense of what you are thinking and doing, especially in the

context of your – the week ahead vis-a-vis application penetration, sort of the next or significant threat area and one with I think even more significant privacy considerations?

Mr. Brown: So the easiest way for us to try to address that is by expanding our working our relationships with the private sector. And it's -- I think an example is the last couple of months the major zero day vulnerability on – that a lot of press and got a lot of attention and a lot of focus on both the federal and the private sector side, but there was an application issue that, frankly, we could address. We needed to rely on the individual software provider to try to come up with, you know, capability.

And for them to provide us the information that allowed us to understand what the vulnerability was, not only to mitigate it, but so that we could see what the potential operation effect was.

This is a very difficult effort. It's things that we've tried and started underneath both the CNCI Project 12 Public/Private Partnership, but

there's another element that we have, which is called the Enduring Security Framework, which is again part of the Public/Private Partnership. Senior CEO's of the private sector working with the senior government officials from Department of Defense, DHS, DNI to address hard problems like this and figure out why they're hard.

If it's technical, you know, we're going to have to vet the technical piece, but that's usually not the hard part. It's the policy, the legal, the other barriers, competition and propriety information that we're handling as the government working with corporations that the corporations are trying to figure out how they work in a non proprietary environment, where everything is proprietary.

Mr. Purcell: Okay. Neville, please?

Mr. Neville Pattinson: Thank you, Mr. Chairman. Question regarding integrity of the audit. And so, you put as you gather information. To what extent are you looking for things inside the users, the user base that's inside the system,

monitoring the system, accessing the system? A lot of this is about intrusion detection from outside. It's going to – breaking in defense of strategy and stopping things from coming in. What have you got as far as the impact for the people that are actually online? Does this HSPD 12 have an impact to what you're doing? Or you know, what's the ability to actually understand who's accessing the data and why? And how is that been recorded in the audit world?

Mr. Brown: So it's – a couple of answers there. And that was the other one you asked about, which is CI. So there are several things that we as the U.S. Government, and just the 12 being one of the examples, that we're trying to address potential insider issue, whatever the insider is trying to do. So there's a, first of all, you've got HSPD 12. You've got initiative 6, which is focused on counterintelligence, so that the law enforcement counterintelligence personnel are putting out additional tools and capabilities on all of our networks and increasing the analytic capability to

be able to look for potential insider threats.

But then on the – for our responsibilities inside DHS, in fact, this mission, we are looking at trends. So we're looking at whether the other departments of the agencies are reporting to us as incidents. And digging deeper at a real tactical level at the auditing procedures that we put in place, that is focused on our individual users enable us, because they access the information and data from our tools, like EINSTEIN 2, when we get to EINSTEIN 3, like EINSTEIN 1, to make sure that they are acting in accordance with standard operating procedures that we've got. And then at a higher level, it's more – getting the right training at an appropriate time, the other things. That – those are some of the things that we've put in place, both as the Federal Government and individually in our mission statements.

Mr. Purcell: Thank you. Larry, you decline your opportunity here?

Mr. Lawrence Ponemon: Actually, I have another question.

Mr. Purcell: Then you're next up.

Female Speaker 1: Mr. Charles turn next?

Mr. Purcell: I know, Charles is next. I've saved the best for last.

[laughter]

Larry?

Mr. Ponemon: So second best, is that what you're saying?

Mr. Purcell: No, no. I'm sorry, Jim was yesterday.

Mr. Ponemon: Much appreciate it. Thank you. You just focused on the danger of public and private partnerships, when you see the kinds of change. For example, we see an operation of war. We see different types of attacks. And by the time you get a signature, it's really too late. At that point, is there penetrating, you know, it's more then government it's everybody, every invitation.

Do you have the strategy that (coughing) signature before signature saying networking intelligence strategy network? Is that part of something that you're operating? And then part 2,

do you have enough resources to get that work done?

Mr. Brown: (Inaudible).

[laughter]

But that's part of what we've been doing over the past two years. I mean, that's – I've been at DHS for 22 months. When we got there, we had 28 Feds inside NCSD. We've got 162 as of Monday and another 51 in the pipeline. Still not nearly enough that we can teach and deploy capability because you're seeing a lot where they – Part 1, as part of our responsibilities with respect to the private sector, we work with the identifiers, vendors. We work with the software producers. We have different relationships with different companies.

And part of what that is about is to – if there is inklings, if there is the sense that you've got a zero day, you know there's a zero day, you know there's something else that's out there, working together and recognizing proprietary situations that you're in, that when it's appropriate and that we've got capability, we try to get that information out.

And we try to do it in a way that we can get it

out as quickly as we can, not just to the federal departments and agencies, but again, easiest for us is to get to the sectors, to get to the second calls. So we have established – and that's not good enough. So the other things that we've done is building up a process that the DOD has with the defense industrial base, which allows for the bilateral sharing of information, in order to find out some of those threat vectors, we rely on what the private sectors, they might be seeing first. And so, we're – we have done – started a pilot in the financial sector, looking at continuing to do that with the ICT sector and energy sector, because of the smart grid coming.

We have long established procedures in what I'd say that comes with everything is trust with these sectors with the departments. So that trust rests upon the ability for them to provide us information that we – that they know we will not inappropriately disseminate.

And so again, that gets back to our policies and procedures at different points. But the bottom

line, we are not capable of operating at Internet speed at this point. We're doing a lot to close that gap. But in order to be successful, it calls for that public/private team to be working together. And that's why I think – everybody's on board. It's getting over that parts.

Mr. Purcell: Thank you. And Charles?

Mr. Charles Palmer: Yes, thank you, Rear Admiral for your remarks. The Public/Private Partnership is vital. We have to have it. You can't do it alone. And neither can the private sector. But you both have one problem, that is workforce. How do you find the people to help you do this?

My question is the same question the rest of industry is asking. Where are going to find these folks? Is DHS doing anything to try to stir this up and make it a desirable career?

Mr. Brown: I love my job.

[laughter]

It's the workforce is probably not the biggest we've got. I think I just got quoted in another

magazine saying something like that. So DHS, I mentioned initiative 8. It's not nearly enough for the Federal Government. It's Initiative 8 underneath the CNCI did not address the private sector side. So what we've been doing for the last six months has been expanding Initiative 8 so that we can address it as a national issue, and bringing in the Department of Education, and bringing in and building off of some of the things that we at DHS, that folks don't know about. 106 – we have relationships with 106 universities and research centers to try to expand competency in cybersecurity, in cyber operations, cyberspace, computer science. We have the scholarship service. All of those, I think are just – are foundational pieces of how we can approach to expand (inaudible). So we're trying to – through several vehicles in the interagency, DHS, taking the leadership, expanding our roles. And late last night, Mary Ellen called me out of the budget meeting, was that we built towards the next budget FY '12. What DHS can take as a significant leadership role with respect to

training and education. So all of those are part of it. We've also got the Secretary announcing Site Security Awareness Challenge at RSA, which is hey, I tell my wife I'm smart, but by no means smart. So the idea is to take all the smart people out. What are the potential solutions to this? That's part of what the Secretary's looking at. And then, we can try to roll that in into not just awareness, but how we can attack the education and training aspects of this. Huge confusion.

Mr. Purcell: Admiral Brown, thank you very much for your time today.

Mr. Brown: Thank you.

Mr. Purcell: We appreciate it. And we look forward to hearing from you again in the near future.

Mr. Brown: Thank you.

Mr. Purcell: And best of luck. Thank you.

[applause]

At this time, what we are – we're looking at a break, which I'm sure everybody is delighted by. I wanted to first thank Mary Ellen Callahan and

Admiral Brown for their comments, their availability. We will be following up, as I said earlier, with some questions from the Committee to Mary Ellen. And we'll figure a way during this 15 minutes to slot that into our schedule.

Please return to your seats in – do we have 15 or 15 minutes? So at 10 after the hour then, please.

[break]

Mr. Purcell: Thank you. As I mentioned at the outset of the meeting, again, please silence your mobile devices. And also, those that wish to address the Committee, there's a sign-up procedure. The sheets at a table outside of the door. We welcome your comments. So please, take advantage of the opportunity, if you would.

It is -- it's a distinct pleasure to invite our next guest. And it is also a -- as was expressed earlier, somewhat bittersweet. Toby -- Toby Levin has been a -- I'm trying to avoid certain words, words like fixture.

[laughter]

Ms. Levin: Good idea.

Mr. Purcell: Toby Levin has been an integral part of the privacy dialogue for a very long period of time and, in fact, is easily considered a pioneer in -- in privacy and data security policies and procedures, both in the public and in the -- in -- in the private sectors. Personally, I've -- I've known Toby for a long time, and met under excellent circumstances at the Federal Trade Commission. Enough…

Ms. Levin: We couldn't have done those workshops without you.

Mr. Purcell: … enough years ago to where we -- - we both prefer to gloss over that part. But -- but it -- it is -- it is a real distinct pleasure to -- to welcome Toby to address the Committee. She's been with the Department at the Privacy Office for -- - for at least five years now. And everywhere Toby's gone, she's influenced the -- the – both the policies and procedures at that Office in rather profound ways through a passionate approach,

dedicated work. And you know, all of us admire her unflagging kind of work ethic as -- as -- as she -- she goes through these very hard issues.

So we're delighted to welcome her. And following her remarks, we're going to go through hopefully a little bit of a love fest with Toby. And I invite the Committee members to begin preparing their glowing remarks now. Yes.

Ms. Levin: I want to put it on a C.D. and give it to my kids.

Mr. Purcell: Toby, welcome. Welcome.

Ms. Levin: Thank you. Well, it's my great pleasure to brief you this morning. I've known, I think, most of you for a number of, number of years, and really value the work that you have been doing for this Department, but more broadly, for privacy generally for -- for your careers as well. Thank you.

I'm going to brief you this morning on the work of the DHS Office and its interagency activities, particularly with the federal CIO Council through the Privacy Committee of that

Council. And let me first give you some background about the federal CIO Council because I don't know if everyone is familiar with them.

The -- our own Chief Privacy Officer, Mary Ellen, is one of the three co-chairs of the Privacy Committee of the federal CIO Council. The other co-chairs are Nancy Libin, who's the Chief Privacy and Civil Liberties Officer at DOJ, Department of Justice and then Roger Baker, who is the Assistant Secretary of Information and Technology and CIO at the Veterans Administration.

The Privacy Committee is one of five sub --five committees of the federal CIO Council. And the CIO Council was first established by an executive order in 1996 and then later was codified by Congress as part of the E-Government Act of 2002.

The federal CIO Council serves as the principle interagency forum for improving design, uses, sharing and performance of federal agencies information resources. And the council makes recommendations to OMB on IT investments, policies, procedures and standards.

The executive leadership of the CIO Council includes the Deputy Director for OMB, who is Jeffrey Zients, serving as the Council Executive Chair, which means he's not there at every meeting, but he has that post.

The Federal CIO and OMB Administrator for e-Government and IT, who is Vivek Kundra, serves as the Council Director and the Vice Chair, who's elected by the members of the CIO Council and from that membership. And currently, that's David Wennergren, who is with the CIO -- Deputy CIO at Department of Defense.

So the members of the CIO Council are the CIO's and deputy CIO's of the federal -- executive federal agencies. And our own Mary Ellen Callahan serves on the CIO Council Executive Committee.

The five committees of the CIO Council are divided into Architecture and Infrastructure as one, Best Practices. Third is Information Security and Identity Management; fourth, IT Workforce, and fifth is the Privacy Committee. And that is the one that we have been very actively engaged in.

Membership on the five Privacy Committee includes the Senior Agency Official for Privacy and Chief Privacy Officer in federal agencies. Now, some of you may not be familiar with the term Senior Agency Official for Privacy. That's SAOP, or S, A, O, P. And OMB Memoranda for those of you who like citations, M0-5-08 in 2005 called on all executive departments in the agencies to identify to OMB the Senior Agency Official for Privacy issues and policies for that agency.

And many cases, the Senior Agency Official for Privacy is the CIO for that agency. But he or she may also have a Privacy Office, a Director of Privacy, within the CIO operation.

In other agencies, it’s a dedicated individual, a Chief Privacy Officer. And as you know, Department of Homeland Security, Department of Justice, and now HHS, Health and Human Services, have mandated congressionally mandated Chief Privacy Officers.

The Privacy Committee provides interagency support to OMB and serves as an interagency

coordination group for privacy issues. It provides a forum for privacy leaders within the federal government to advance best practices, promotes privacy policy and protections throughout the Federal Government.

The Privacy Committee meets at -- on a -- on a monthly basis. And many members of the privacy -- DHS Privacy Office have had the good fortune of being able to serve on the various subcommittees of the Privacy Committee.

Staffs of the -- staffs of the privacy offices and -- are invited to be the members of the subcommittees of the Privacy Committee. Lynn Parker, Mary Ellen's Executive Special Assistant, serves as an Executive Assistant to the Privacy Committee in helping to do minutes and other important recordkeeping for -- for the Committee.

The Privacy Committee is divided into five subcommittees. Best Practices, Development and Education, International Privacy, Web 2.0 and Identity Management. Let me just briefly describe what these subcommittees are -- are doing.

The Development Education Subcommittee serves as a forum for educating federal employees about privacy laws, regulations, policies and procedures. And its primary responsibility has been to serve to set up and develop an annual privacy summit, which is held in the fall. And it has been a wonderful experience helping to form the agenda and -- and see the turnout and response of federal privacy employees.

We have a standing room only event. It's been extremely successful. It's only open to federal privacy professionals. And there was a parallel event for the IT community. And ours has actually been more widely attended by our community and has been a great success.

The Subcommittee is also creating a clearinghouse for federal privacy agencies on resources, materials, and training opportunities. So our -- at the DHS Privacy Office, our Associate Director for Communications and Training, Steve Richards, who joined our staff back in -- earlier in the fall, is participating on that Subcommittee.

The International Privacy Subcommittee serves as interagency forum for agencies that are interested in U.S. Government privacy framework and development and how it affects U.S. Government interactions internationally. The Subcommittee focuses under -- international data privacy standards and new developments in that area in supporting existing processes established by large, coordinated, consistent message on privacy from U.S. Government agencies.

And I'm saying it that way to make sure that everyone realizes it's not setting international privacy policy for the U.S. Government. It serves as a forum for the professionals, privacy professionals who are dealing with those issues to come together to discuss the -- what's happening -- what's happening on the international front, and -- and to make sure that they're having -- developing consistent messaging. The -- our own John Kropf, Deputy Chief Privacy Officer at DHS, serves as one of the co-chairs for that Subcommittee.

The Web 2.0 Subcommittee provides a forum for discussion and recommendations on best practices to promote President Obama's open government transparency initiative while protection privacy. It's been working on various social media implementation issues, including drafting model PIA and SORN for social media for federal agencies.

The -- the newest subcommittee is the Identity Management Subcommittee. And it's working with the CIO Council's Identity Credential and Access Management Committee, known as ICAM, to develop implementation guidelines and profiles for federal agencies' use of federated identity credentials created by industry groups. And this was in response what Richard said earlier, his interest in that area.

Its work is posted on the -- on the federal identity management.gov Web site that's idmanagement.gov. And there you can see in the ICAM area the roadmap and -- and process publications with regard to the use -- government use of federated identities.

The Subcommittee is now reviewing applications from federated identity frameworks and is developing a model privacy impact assessment for use by federal agencies when considering how they are going to use federated credentials on their Web sites.

The ICAM documents include a trust framework provider adoption process for privacy -- trusted privacy frameworks. And it includes criteria, specific privacy criteria, that we helped to develop that must be met by these frameworks. And I can talk a little bit more about that, if you -- if you like.

The -- the last privacy committee is the standard and standing privacy subcommittee. It's the Best Practices Subcommittee. And I have been -- have had the pleasure of co-chairing that Subcommittee.

It serves as a forum for development and promotion of best practices for privacy programs and policies. It engages other members across the Federal Government who want to consider how we might

further the guidance on implementing privacy best practices. And it works with the -- also with some of the -- some of the CIO Council subcommittees as well where we have joint issues.

We look -- for the past year, we've been particularly focusing on several challenging projects that build on the eight fair information practice principles, which I know members of DPIAC are very familiar. For those in the audience here, the eight fair information practice principles that are the policy for the Department of Homeland Security include transparency, individual participation and redress, the purpose specification, data minimization and retention, use limitation, data quality and integrity, security and accountability and auditing.

So this Best Practices Subcommittee has taken those principles and is looking to see how we can embed them in, for example, the federal enterprise architecture. And for those of you who -- - of the Committee will be looking at -- at SOA's in your next document coming up, that, too, is part of

this federal enterprise architecture that is the -- the way in which IT investments are supposed to be evaluated.

And it's really the building blocks of our -- of our data systems, our information systems and across the Federal Government. And we're looking to include privacy principles and fair information principles as building blocks within the enterprise architecture.

We meet basically every other week. So it's a significant time commitment. We have several deliverables that we're working on that will help provide guidance on implementation of the fair information practice principles.

We'd like to think in some ways that we're following on the -- in the footsteps of an organization like NIST, which -- National Institute of Standards and Technology, which provides significant guidance to the IT community, the federal IT community on information security practices. The privacy community has not had the good fortune of a similar type of organization.

We don't have that library of resources and documents that NIST have. But the Best Practices Subcommittee is seeking to develop similar types of materials to help further implementation of privacy within the Federal Government.

In addition, we have an ad hoc working group, which is now focusing on the privacy issues associated with cloud computing. And DHS staff is involved in that working group along with members from subcommittees of the CIO Council and staffing from GSA that are looking to identify the privacy issues associated with cloud computing and how to propose steps to mitigate those risks.

So I think -- and frankly, in every area of privacy that you can think of, the DHS Privacy Office has its staff involved in an interagency way trying to help set -- provide leadership and help set policy in the Federal Government in that area.

In -- and just in conclusion, as you know, I am retiring. I have to say that this last year my experience working with the Privacy Committee has probably been one of the most rewarding, both

because it's -- I've been able to work with so many dedicated privacy professionals in other agencies, but also because I see that we have an opportunity here to really build some excellent resources for the federal privacy community through this interagency work.

I'm sure that the work of Privacy Committee will continue to -- in a very concrete way to demonstrate leadership within the federal government in the privacy area. And I'm happy to respond to any questions that you might have about the work that we've been engaged in.

Mr. Purcell: OK. Thank you very much. I'm -- I'm -- it's heartening to hear that the federal government agencies have such a collaborative approach. This assures or at least enables a far more harmonized approach to that protection and -- and information privacy than many, many, many other organizations across the planet.

And this is a -- you're miles ahead of -- of where you've been. So thank you very much for -- for the briefing, but also for the effort that

you've put forward to herd all of these cats into this kind of cohesive form.

Committee members, I'm sure you have some questions. Please, if you would, turn your tents slightly toward me, so I can see not just a blank white tent, but -- like that, John.

[laughter]

And so, we'll start with John.

Mr. Sabo: So, starting with me, Toby, just a -- just comment for the working committee. You made the comment that your -- your -- huge library of standards and work, and papers and research with that on the data security, information security practices, standards, cryptology, et. cetera, cryptography. And we don't have that as at ours. But I just want to make a point for the record and then you won't be carrying on your work for DHS --. And that is that we're seeing customer focus now -- focus on smart -- receiving more attention in the standards community developing those libraries.

Ms. Levin: Right.

Mr. Sabo: And I've really -- and I've spoken to

several of your -- some of your colleagues. I think it's important to add either work -- migrate and take advantage, leverage -- committees, whether it's happening in the oasis will happen -- and other bodies of committees of HHS -- privacy -- stronger engagement it's not appropriate to DHS -- and miss response -- privacy reference model --.

So I think there's an opportunity to do more to promoting those standards -- . And I just wanted to make that comment.

Ms. Levin: Well, I think that's very important. And the Best Practices Subcommittee has been working closely with Ron Ross at NIST. We very much value his expertise. And he personally has expressed strong interest in working with the Privacy Committee in -- in making sure that we bridge relationships with the IT community and we embed privacy into IT considerations.

And as we work on, for example, the enterprise architecture and other projects, we want to make sure that everyone understands that it's the privacy professional that will bear the

responsibility, the real responsibility for embedding privacy. We don't want the IT community to think that that's their responsibility, that we're just giving them more work to do, or that they're experts in how the privacy issue should be done.

But rather, we see that it's a -- there's very important partnership that has to happen and that we can actually make sure that privacy is built into what we refer to as a system development life cycle and into IT development considerations if we're there as partners.

Mr. Purcell: Thank you.

Lisa Sotto?

Ms. Sotto: Thank you very much, Toby. And thank you for the work that you've been doing and will continue to do it. -- my question -- your -- your comments just now.

I'm curious to what extent the CIO Council -- - privacy as something that is distinct from information security and -- and that's bigger than just computerized electronic data.

Ms. Levin: Well, I think there's -- I think the -- the awareness varies from agency to agency. But certainly, in our agency and the ones, I think, where you have the most active privacy offices, they're very aware.

We have -- just yesterday one of the key members of the CISO staff was in our office talking about issues. They're -- we're constantly recognizing each other's role where we are involved in projects and we say, oh, we need to be sure that CISO's involved. Or the CISO's involved in something, and they say oh, we need to make sure that privacy's involved. And they recognize that we have other, you know, separate areas of expertise.

I think it may vary agency to agency, depending on the strength of the offices. And in some agencies, the privacy official or the privacy officer is -- sits within that office. And -- and it -- it may vary in terms of what those relationships are. But I think where you have the -- the stronger privacy offices, that clearly, their -- their distinct roles is recognized.

Mr. Purcell: Thank you.

Charles, you've removed your question, right?

Mr. Palmer: Yes.

Mr. Purcell: OK. Fine.

Ramon?

Mr. Barquin: First of all, Toby, and Mary Ellen, I think this is a fantastic effort. I've worked with the CIO Council on a number of issues over the years. And it's a very, very, I think, good forum to work with. I would…

Ms. Levin: Ramon, I'm having a little trouble hearing you. Sorry.

Mr. Barquin: Well, all of that was just complimenting you guys.

[laughter]

But the -- no, the -- the question is you -- you mentioned about the -- the importance, well-recognized, of looking at privacy considerations when you're dealing with enterprise architecture, specifically SOA, which as you know, we've been working on. And one of the questions that we get

asked by the CIO within Homeland Security was what outreach have they done to see what was going on in other agencies, other federal agencies?

So the question -- because they didn't know. And now the question is to you. Who else is doing work within other agencies looking at privacy considerations related to enterprise architecture, specifically SOA?

Ms. Levin: I can't tell you that I -- I know what other agencies are doing. What I can tell you is that within the Best Practice's Subcommittee -- and I guess I can -- all right, let it go.

There is a product. It's called the federal enterprise architecture security and privacy profile that is in the last stages of review by the CIO Council members through -- by the CIO's, that OMB hopefully will release when that process is completed. And that profile, I think, will play a significant role in -- that our Subcommittee helped develop.

We did the privacy portion of it -- will -- will make a significant contribution to all

enterprise architects to say here is what you need to look at when you're thinking about security and privacy. The security piece is no surprise. It's -- - it's built on the security control families that are set out in a NIST publication, 800-53, that were originally identified in -- in FIPS publications 199 and 200. So they have a long -- as I said, a long body of -- a long history of -- of identifying what are the security controls.

Well, what we have done on the privacy side is we've established the eight fair commission practice principles as the control families. So that when enterprise architects work with their IT people and their privacy professionals and their program business owners to identify -- you know, to say well, what are -- what are the privacy roles, responsibilities that need to be built into the architecture, they will look at these eight control families, which are the FIPPs, which are rooted in the Privacy Act, the Government Act, and -- and privacy best practices.

So I think that -- when that document

comes out, I think that will basically be the -- the demonstration that privacy is part of the enterprise architecture. And what -- what architects, business owners need to look to are these principles, which are then called control families.

Mr. Purcell: Joe?

Mr. Alhadeff: Thank you.

The -- the first part would obviously be to endorse all the wonderful things Richard said and just indicate that they're probably inadequate, but they were as good as we could expect right now.

[laughter]

The second is really a two-part question. And -- and we can repeat that for Mary Ellen when she comes back, if that's useful.

The -- the second is, especially for two of the committees, the Web 2.0 and the IDM Committee, one question is to what extent is there outreach to actually private sector experts in those Committees because they will be foreshadowing some of the technologies that may be used. So in order to keep abreast of the developments, it may be useful that

there are some aspects of public, private interaction related to those Committees, although not standing memberships, but rather consultations as appropriate to make sure that people are abreast of the -- the latest developments.

And then the second question is, as we look -- you mentioned a lot of the life cycle issues and the fact that the CIO Council is involved in those. And even when you get to such a highly strategic member of an organization as the CIO, you are still talking about a technical implementation at that point. Whereas some of the privacy issues we are discovering as we look at privacy by design in the private sector need to be considered before you get to the consideration of the technical issues at the consideration of how you articulate what's the need and the -- the movement of the organization.

And so, the question is is there anything going on at the level of the Committees that helps also address that need to have the conversation going on before you get to the technical components, but in the expression of needs, to make sure that

those are done in -- in a way that is narrow and compelling and it achieves the needs of the organizations, but in a way that is most respectful of privacy.

Ms. Levin: I think there is a recognition that those discussions have to happen at the earliest stage. And I'll just give the example on cloud computing, where the working groups include, you know, experts from NIST and federal agencies and the privacy -- federal privacy leadership. And -- and in the discussions about well, what should the security -- you know, basic security requirements be, what should the privacy criteria be, that discussion is happening before anything is being put -- put forward as the -- here is the policy or before there's anything in terms of IT development.

Obviously, there's -- and this goes to your other part in terms of, you know, is there a communication discussion with private sector. It's always -- it's always a challenge to figure out how that discussion takes place. All of the people

involved, I think, are very well-read. And they understand these issues.

It's -- as government, we can't go speak with -- single out particular companies for special relationships because that's not ethical. We can't go down the track of a particular company and -- and go behind what is public and use them as a model for trying to understand what the rest of companies are doing. We just can't do our work that way.

But having said that, I think there's -- there are discussions that happen in public settings where we are, you know, very aware of what concerns or -- or policies companies have that make them public. But I think, more importantly, I think government experts know what the issues are. And we know what some of the basic requirements are for IT security for privacy.

We don't need to -- we don't really need to ask the -- the private sector what are the privacy protections. We know what they are.

The question that comes in, I think, is how do they -- how do we implement them in a way that

works for the government, public and private sector. And, for example, I'll use the project where we've worked with the Identity Management Subcommittee that's been working with ICAM on federated identities.

There was a lot of outreach to the trusted framework provider groups. You know, Open ID, Kantara, Info Card, the groups that had come forward to say we are interested in -- in government using these federated identity -- these federated credentials. And we're going to provide a vehicle for evaluating and assessing specific identity providers' ability to meet certain criteria. But it is the government that set up the criteria that these framework providers need to meet.

As of now, open identity exchange and Kantara initiative have provisional approval from the -- the ICAM project, from the ICAM group. And that approval was based on criteria that were published -- public. And our Subcommittee participated in -- in including specific privacy criteria, which on that identity manager ID manager

Web site, the trust framework provider adoption process document on page 12 lists the trust criteria, which are opt-in, minimalism, activity tracking.

They address activity tracking, adequate notice, the fact that the credentials -- this is from the government side -- cannot be compulsory. The government will need to provide alternatives for people who don't want to use federated credential and what would occur in termination.

Now, these are just very broad criteria. More -- more guidance, I think, will be developed in time. But at least they're there at the outset that any trust framework provider, if they're going to be -- if they're going to be approved for -- for use by federal agencies must provide an opt-in, must transmit only those attributes that were expressly requested.

And they have to be consistent with the PIA that agencies are asked to do or will need to do when they're implementing these credentials. And it also tells the identity provider that they must not

disclose information on the end user activities or use any information that they gather for any purpose other than just to provide the federated authentication. And so, there are some basic criteria.

Now, each agency will need to go ahead and do their own PIA as far as their own implementation. But it's very important, I think -- in that process, there were discussions with these outside framework providers to find out, you know, what they -- what their capabilities were, what their -- what they wanted to achieve. And then can they actually meet these criteria?

And the ones that are are being provisionally accepted. We're going to -- there's more work being done on the fact that these providers are going to be using audit firms or assessors to evaluate whether or not their identity providers are actually meeting the criteria. And we're going to be developing some guidance specifically to the auditors about what they need to look for with regard to privacy implementation.

So -- so there needs to be that dialogue. But ultimately, it's the -- it's the government that has to decide the criteria. And I don't think we -- we -- it's not a negotiation in that -- in that regard.

Mr. Purcell: Thank you.

Joanne?

Ms. McNabb: I will be quick. Are any of the Privacy Committee materials available online in the same way that the I.D. management stuff is?

Ms. Levin: Well, our…

Ms. McNabb: Available to me.

Ms. Levin: Right, the one -- we have not yet published any of these -- of the documents that we -- we're working on. They're now in the process of going through going approval.

Ms. McNabb: OK.

Ms. Levin: But the documents on the ICAM, specifically the roadmap and the application -- adoption process reflect -- anything you see regarding privacy is work that reflects our -- our contributions. But we will be publishing our

deliverables as they go through, once they complete the review process.

Ms. McNabb: Thank you very much. And also, Toby, thank you for your service, to Americans as consumers, when you were at the FTC, and to Americans in general at Homeland Security as well as non-Americans who come here. You've been such a staunch and intelligent advocate for public interest. I really appreciate it.

Mr. Purcell: And David?

Mr. D. Hoffman: Yeah, I would like to follow up on what John was just talking about. Toby, I had the great fortune -- I consider myself really lucky to have known you and had the pleasure to work with you for close to a decade now. And in your career at the FTC and at DHS, in my opinion, the combination of your tremendous intellect, your energy and the high level of integrity and personal ethics with regard to your work has been unparalleled. It's been absolutely fantastic.

And I just wanted to take a couple moments to note some of the things that I think are just --

just tremendous of what you've accomplished that I'm not even sure you may recognize that you accomplished. I think your ability to focus, not only on the mission of the organizations that you've worked for, but then also with respect to individuals' rights and not be balancing those two against each other, but find creative solutions to accomplish both has been something that you've been able to teach a great number of people on how to do that.

I look at, you know, the impacts you made at the FTC. I mean, going back to COPPA. And -- and then, onto the -- what you did at DHS, I think the work you did on the FIPPs at DHS is going to live on and be a tremendous legacy and an impact that you made.

But I think the biggest impact that you made is that you acted as a leader by example to a whole generation of privacy professionals on how to do their job. And I consider myself to be one of those folks who learned how to do his job by watching you do your job. So I want to thank you as

a citizen and for what you did for the country. And I want to thank you personally for what you did for me.

[applause]

Mr. Purcell: Thank you very much. We're good.

Ms. Callahan: Little known fact about me -- I cry whenever I see anyone else cry. But thank you, Toby.

Because really -- I think, David, you summarized it better than I can. And she really has been an amazing leader.

So thank you for everything.

Mr. Purcell: Thank you.

One of our -- one of the really pleasurable duties of the Committee is to develop points of view to -- and recommendations for the Privacy Office.

It is a real pleasure to present today a discussion of two of those papers that we've presented in draft form here. So we'll turn to those reports from our Subcommittees.

The members of the Subcommittees have proposed recommendations in two areas. One is in the implementation of enterprise service bus infrastructures for software-oriented architecture and supporting services.

The other is in the area of the elements of redrafts program. We would like to == to note here that the Federal Advisory Committee Act requires the subcommittees to present their proposals to the full committee to deliberate those -- the points made and the recommendations and -- and conclusions and to decide whether or not to adopt those recommendations, either as proposed or as amended.

We have distributed the papers to our Committee members. And I'll call upon the Subcommittee authors to present their summaries of those papers, to explain the recommendations and to -- to conduct -- or to ask for input to the content of those papers and the recommendations and any potential for amendments or additions or revisions.

We will then have those discussions. And

we will vote to approve the amended versions of those -- of those papers and submit them to Mary Ellen Callahan and the Privacy Office.

So first, I would like to -- to turn to Charles Palmer or your designate?

Mr. Palmer: Yes. Ramon's going to give the summary, and I'm going to take the notes for all the changes.

Mr. Purcell: Fine. Ramon, then. Ramon Barquin, the data privacy -- I mean, the Data Integrity and Information Protection Subcommittee has -- is offering a paper on recommendations for the PIO process for enterprise services bus development. Can you please lead the discussion?

Mr. Barquin: Sure. First of all, it needs a -- couple of minutes of background. As the departments of CIO started to move towards a services-oriented architecture, a SOA, it became rather clear that there were significant privacy implications that were involved with the SOA. So we were asked to start looking at these. As we had several meetings with the Office of the CIO, it

became very clear that they were moving at a speed where the principle focus of their work was on developing either an enterprise, a single enterprise service bus or a collection of component buses that would serve like an enterprise service bus.

Hence, we agreed that the most useful set of recommendations for us was to focus on that enterprise service bus and looking at the PIA process for that bus development. And that's what you have in front of you, for the rest of the -- of the Committee. With that just basic background, what we did was significant things.

First, we incorporated, as Toby has done with that FIPPs, you know, security and privacy -- we incorporated the FIPPs, the fair information practice principles, into -- into the part of any -- - of any ESP implementation.

We also brought attention to the three most significant categories of privacy risks in ESP implementation -- being, first of all, access control, controlled access by individuals to the bus; second, policy enforcement and policy

enforcement in the sense that since the whole reason for SOA is to have services interconnect them, the bus if the primary mechanism for transporting, you know, the data between those services. It's policy enforcement related to what connects, how it connects and what is allowed through that bus.

And third, and also very, very important is auditing, the ability to go back and be able to audit and hence, enforce policies, et. cetera. So those three are the principle privacy risk categories that we pointed out.

And then related to that, we actually made a series of recommendations. There are six specific recommendations that go along with our -- our study of -- of this issue. And those are specific recommendations dealing with privacy and the bus.

We also added at the end a series of questions more than anything else that had to do with the fact that, you know, the -- the bus isn't being developed from scratch, in a sense. There are already a number of existing component buses that are being brought together interlinked, you know,

into a DHS bus. So we've provided a series of questions that we thought were important to be asked about those existing buses in order to incorporate that into the PIA for that enterprise bus and likewise, a -- a number of considerations related to planned services around that bus.

So that gives you the 100,000 foot level of the -- of the paper that we've produced. And the question now is, comments.

Mr. Purcell: Thank you, Ramon.

You've had a few days to examine the paper. I hope that you've taken that opportunity to give it a thorough reading. At this time, I'd like to open the floor for discussion points from the members of the Committee about any particular area of the paper that you want to comment on, challenge or -- or question.

John Sabo?

Mr. Sabo: Yeah, a couple of comments and observations for -- regarding the paper. And it's a very good start. A couple things stood out. It seems to me at times that it's not entirely clear if

it's aimed at the developers of the PIA model for SOA or if it's aimed at the developers of the -- of the architecture itself.

And I'm not -- and it isn't just wordsmithing here. I think if you look at the recommendations, if -- if a developer of risk policies and procedures to qualify individuals and servicers requesting access to ESB, which is clearly a recommendation, is that aimed at let -- in other words, is that aimed at the developers of the PIA model? Or is that aimed at the developers of the architecture?

And I think the way to -- so I think a little bit of wordsmithing to say the overall -- I mean, I don't have the language here. I have some suggestions. But overall, the thrust of this is to say when you're doing this bus, these are the key recommendations associated with it. And developers of the PIA need to include the consideration of these recommendations in the PIA development process. So that's a comment. I'm not sure you all agree with it.

The second thing is there's a very big focus, which is very appropriate, on policies and procedures. But a SOA is by, almost by definition, going to be an IT implementation of those policies and procedures. And so, I would recommend adding a phrase such as a technical mechanisms and controls in a number of places where there's a reference to policies and procedures, because if you're going to do -- if you're building a PIA, it seems to me in today's environment, the network environment and so on, that -- that you shouldn't overlook the criticality of evaluating the technical aspects of that architecture and not simply --.

So, for example, in recommendation one, one could add developer risk policies and procedures and technical mechanisms necessary to qualify --.

In recommendation three, develop policies and procedures -- again, I would add technical mechanisms.

And one last comment is just a minor, tiny wordsmithing. But under recommendation two, we don't define terms with less robust process, even

though it may be a mini PIA or a subset of the PIA. I'm not sure less robust is appropriate there. I think we're a robust process for what we're targeted the PIA may be. So those are a few specific comments for you to consider.

Mr. Barquin: First of all, I think your -- your first comment is -- is right on the mark. We were talking to the developers at the CIO. And yet, the -- this paper should be, you know, for the PIA. So we -- we will do some of that wordsmithing. I think that's very important.

And I wish I were less robust, but -- but I understand we ought to change that word to…

Mr. Palmer: I didn't quite understand the less robust comment?

Mr. Barquin: You know, that if you have a process in place, less robust is probably not the best way to describe what we really mean, which is a -- one that will take less effort to produce.

Male Speaker 1: Yeah.

Mr. Sabo: As opposed to…

Male Speaker 1: Less cumbersome or

something.

Mr. Sabo: That's right.

Male Speaker 1: You don't want to say that.

Mr. Barquin: And the technical mechanisms -- you're absolutely right. We'll -- we'll that stuff in.

Mr. Purcell: We'll add it now.

Mr. Sabo: Yeah, yeah.

Mr. Purcell: So may I suggest then a wording change under both numbers one and two that following policies and procedures, that -- I'm sorry, one and three -- following policies and procedures you include and technical mechanisms and controls as a phrase. All right?

Male Speaker 2: Right.

Mr. Barquin: Is that acceptable, John?

Mr. Sabo: Yeah.

Mr. Barquin: OK.

Male Speaker 2: Number four as well, Richard?

Mr. Purcell: Wherever you have policies and

procedures.

Male Speaker 2: Global search and place.

Mr. Purcell: Fine, fine, yes, number four as well. Fine with that.

Mr. Barquin: The -- and -- and under number two, may I simply suggest that we revise to say such a process may be more targeted and leave it at that? Is that sufficient for you, John?

Mr. Sabo: Yes, that's great. Thank you.

Mr. Purcell: Are there other comments to the paper?

Let's see, that's Joanne?

Ms. McNabb: These are truly wordsmithings. But if we're going to vote on this today, I think we need to smith a bit. On page four -- so let me make sure I'm understanding this right -- that the first full sentence of the top of the page of my version, which starts with "access controls for individuals," here's what I think this means to say. Access controls for individuals have to take into account the authority of the individual to access the data and the specified purposes for which individuals may

use the data.

Is that what you mean, rather than…

Mr. Barquin: Yes.

Ms. McNabb: Yes. So to access the data…

Mr. Purcell: Access the data…

Ms. McNabb: So we're saying it singly -- and the specified purposes for which the individual -- I guess, because -- may use the data.

Mr. Purcell: I'd like to read that from my notes again, just to be certain of it. Access controls for individuals have to take into account the authority of the individual to access the data and the specified purpose for which the individual may use the data.

Ms. McNabb: Purposes.

Mr. Purcell: Purposes -- may use the data.

Ms. McNabb: And -- and when Charles gets finished with that, I have one on page six in the SOA considerations beyond the ESB, that first paragraph.

Mr. Purcell: Go ahead.

Ms. McNabb: The first sentence after the

semicolon. The other portion, comma, as you have it there -- the services utilizing the data delivery system, comma, also presents -- no, present. No, I'm sorry presents, because it's portion -- presents an opportunity. It's my old English teacher self coming out.

Mr. Palmer: So system, comma, also presents?

Ms. McNabb: Yes, also presents.

Mr. Palmer: Because it refers to portion?

Ms. McNabb: Yeah, exactly.

Mr. Barquin: Well, let's change that to portions in order to leave it.

Ms. McNabb: Well, no, no. There's one portion.

Mr. Barquin: Just kidding, Joanne. Just kidding.

[laughter]

Ms. McNabb: And then in the next paragraph, as it begins, there shouldn't be an apostrophe in individual's. And one more little dinky one -- on page three, at the bottom of the page, the sentence that starts, "therefore qualifying individual access

to an ESP needs to be more rigorous than." You don't need the "that". There's no thing that that refers to.

Mr. Barquin: Where -- where are you?

Ms. McNabb: The bottom of page three, therefore…

Mr. Purcell: Very bottom of page three.

Ms. McNabb: Therefore qualifying individual access to any ESB needs to be more rigorous than -- get rid of the that -- than for.

Mr. Barquin: OK.

Mr. Purcell: Good enough. Thank you.

Ana?

Ms. Anton: OK, so I have been following Joanne's nitpicks.

Ms. McNabb: You got your nits?

Ms. Anton: I have a few, too. So under background on the third line of the -- two to five-year components of approach, you've got -- so under background.

Mr. Purcell: OK.

Ms. Anton: Third line.

Ms. Landesberg: Excuse me. We can't hear you back here.

Ms. Anton: OK.

Ms. Landesberg: Thanks.

Ms. Anton: I'll try to project my voice more clearly. I'll use my outside voice. So background, third line, the sentence that reads "two primary components of approach," I believe that should be "of the approach." Nitpicks.

Mr. Purcell: How about "of this approach?"

Ms. Anton: Sure.

Ms. McNabb: Or this approach.

Mr. Purcell: Good.

Ms. Anton: And in addition to that, on page six, section SOA considerations beyond the ESB. Second paragraph, first line, "we developed these questions specifically for the individuals considering the" apostrophe should be outside the "s".

Ms. McNabb: It shouldn't even be there at all.

Mr. Purcell: It shouldn't be there at all.

Ms. Anton: Or individuals, exactly fine.

Mr. Purcell: Fine.

Ms. Anton: And then another more substantial comment is that in the fair information practices and ESP implementations, there's this bulleted list at the beginning, where it says examples include in that very first paragraph. And then there's purpose specification, data volume, integrity and security. And I would like to encourage -- can I say urge and encourage -- the Subcommittee to perhaps consider actually defining these rather than providing an example because an example leaves things kind of nebulous and could be interpreted in many different ways.

And so, you know, data quality and integrity -- the issue there is that the -- that we want the data that correctly represents the real growth construct to which it refers, not just redundancy. And, you know, I think we should have a real aspirational definition there, if possible. Just a suggestion, but…

Mr. Purcell: Charles, if I may, I -- I

believe that the reason the examples were included - - and it was because the reference to the privacy policy guidance…

Ms. Anton: Has those definitions?

Mr. Purcell: … has those definitions contained. And in prior papers, we've actually used those definitions. And it…

Ms. Anton: OK.

Mr. Purcell: I'm speaking for the authors here, but I believe that there was a certain degree of -- of worry that we were pounding on the definitional repetition in paper after paper after paper.

Ms. Anton: OK, well, in that case, I will propose that we consider the fact that each of these needs to stand on its own…

Mr. Purcell: True.

Ms. Anton: … and that we cannot assume that people have read all of the other recommendations and all of the other documents. And so as an academic, my inclination is to the use definitions that are consistent with the definitions used

previously. And maybe you could just add a footnote to the source of the definition. But I really think it's important.

Ms. McNabb: So for editorial purposes, we could say that you would begin purpose specification, and then use the…

Ms. Anton: Definition.

Ms. McNabb: You will insert the definition that you get from the…

Ms. Anton: Exactly.

Ms. McNabb: … the memorandum, because we know that is, even if we don't have the actual words right at this moment.

Mr. Barquin: Cut and paste it?

Ms. McNabb: Yeah, cut and paste it.

Mr. Barquin: So you want to insert the quote?

Ms. McNabb: The definition.

Mr. Barquin: But the actual…

Ms. McNabb: Yeah.

Mr. Barquin: … you know, quote or the source with a link?

Ms. McNabb: I'd say…

Mr. Barquin: Right the…

Ms. McNabb: … the actual language.

Mr. Purcell: The footnote -- the footnote is the source. And to actually cut out the definition from that source document, paste it in there, and then…

Ms. McNabb: And then give the example.

Mr. Purcell: … then try the example. Is that sufficient?

Ms. Anton: Absolutely. Thank you.

Ms. McNabb: Even though we don't have that actual language for us at this moment, we know what it is.

Ms. Anton: Yeah.

Mr. Beales: Could I suggest an alternative to that? Because I actually sort of like the way this reads. And that is to add the definition itself in the footnote. So it's purpose specification with the footnote, but provides the definition so it's there. And it -- it reads better.

Ms. Anton: So I was ready for someone to oppose that. I was bracing myself for it. So I

still stand with my recommendation, but I believe in compromise. And so, if the Committee believes that that's the best approach, then I would take it.

Mr. Purcell: OK, so Howard, what -- you know, do you have a repost here?

Mr. Barquin: He just said.

Mr. Purcell: Well, no, I know, but if you -- do you feel strongly enough to provide it as a footnote then as opposed to -- do you think it reads better?

Mr. Beales: I think it reads better, but the text -- the text here makes sense. I agree it needs clarification of exactly what we meant on that, but I -- this is not a voting issue with security.

[laughter]

Ms. McNabb: I think it would work as a footnote, as long as it's spelled out in the paper.

Mr. Purcell: We will add it both ways, how's that?

[laughter]

Mr. L. Hoffman: You can't have it both ways to quote…

Mr. Purcell: OK, let's put it -- let's put the definitions directly from the -- from the memorandum, the source document that's listed here and list each as a footnote at the end of that stage then immediately below for reference.

Mr. L. Hoffman: Mr. Chairman, I'm unclear on -- are you proposing to go with the Beales version or the…

Mr. Purcell: Yes, the Beales version is the -- is the pasted footnote.

Mr. L. Hoffman: Including the definition (inaudible)?

Ms. McNabb: Yes.

Mr. Purcell: That is the definition. And leave the examples -- rather than defining them within the text, put them into the -- the definitions into the -- as footnotes for each of the three quoted principles.

Mr. Alhadeff: Richard?

Mr. Purcell: Yeah?

Mr. Alhadeff: Did we actually have closure on the wording for John's issues?

Mr. Purcell: Yes.

Mr. Alhadeff: OK.

Ms. Anton: I want to make a counterproposal.

[laughter]

Ms. Anton: So working a lot with compliance, I think one of the things that concerns me is that people make assumptions about people understanding definitions. So I would like to propose that we consider putting the definitions in the text and the examples in the footnote. And I have a very subtle seconding of that proposal.

[laughter]

Mr. Purcell: Anybody? Ramon, a feeling about this, a desire, a passion over this issue?

Mr. Barquin: I believe that we as co-chairs of the Committee don't care either way.

[laughter]

Mr. Purcell: Would you like to then…

Ms. McNabb: I would prefer putting both of them…

Mr. Purcell: … make a decision? OK.

Ms. McNabb: … rather than that -- rather than

that -- put them both in the body rather than…

Mr. Palmer: Put both there -- nothing more than a footnote is the footnote.

Ms. McNabb: Rather than footnote…

Mr. Palmer: Put both of them.

Mr. Purcell: Fair enough. We're reverting back to the…

Ms. McNabb: Back to the original Anton proposal.

Mr. Purcell: … the principle, followed by the definition, followed by the example.

Ms. McNabb: And…

Mr. Purcell: And you'll author that now?

Mr. Palmer: Yeah.

Mr. Purcell: OK, fine.

Mr. L. Hoffman: And will that also contain, just for completeness -- I think this was Joanne's suggestion, Joanne…

Ms. Landesberg: Mr. Lance, could you speak up for the recorder because we can't hear?

Mr. L. Hoffman: Yes. Is that -- is that just what -- I think this is Joanne's suggestion. Just

what Richard said a minute ago, which was in essence the original Anton proposal, but with a citation at the bottom of a simple footnote to the original source.

Mr. Purcell: That exists already.

Mr. L. Hoffman: That exists.

Ms. McNabb: It's in it.

Mr. Purcell: We're on the bottom of page two.

Ms. McNabb: Opposite or ibid or something.

Mr. Purcell: That's the opposite.

Mr. L. Hoffman: Oh, OK. All right.

Ms. McNabb: I'm not enough of an academic anymore.

Mr. Purcell: We have that. And we will be extracting it directly from that source document.

Mr. L. Hoffman: OK.

Mr. Purcell: The definitions. So we're going to do principle, definition, example.

Ms. McNabb: Yes.

Mr. Purcell: Right? Yes and ibid.

Ms. McNabb: OK.

Mr. Purcell: Good. Acceptable? Any other

discussions?

Yes, Mr. Palmer?

Mr. Ponemon: Actually, I think John is --.

Mr. Purcell: He's had his turn.

Mr. Ponemon: Yeah, this is just a high level and basic issue. When you read the paper, there's nothing that tells a reader why this -- why this particular topic was important enough to study. In the synopsis, you know, on the first page, perhaps you could add a sentence or two why we thought this topic versus the thousands of topics that we could potentially write about, or this particular topic to result in --. So we may know that, but the public reading this paper probably doesn't.

Mr. Purcell: That's a standalone paper. It's -- fine. The -- I had read the first sentence of the background as -- as providing that, but that inquires from your point of view a better detail a motivation for doing this? I mean, is this character development?

Mr. Ponemon: Yeah, just why are we doing this? And why do we see this in coordination? We

don't have to have a rating on this versus the other thousand. But just some description, so that people understand we generally see this as an important issue from a little privacy respect.

Mr. Purcell: Right.

Mr. Ponemon: And I think it's clear to us, but maybe one or two sentences, maybe a paragraph as part of the synopsis would -- and I'm thinking as a former academic. It's probably a good idea to do that.

Mr. Purcell: Fine. I mean, so the entry -- it seems to me, Mary Ellen -- and you can let me know if this is sufficient -- this was a task. So the Chief Privacy Officer of the Department asked us directly to produce these recommendations. And is that sufficient…

Mr. Ponemon: That would be more than sufficient.

Mr. Purcell: … background?

Mr. Ponemon: Background.

Mr. Purcell: Than in the background, the primary statement, or the probably the second

sentence, should indicate that the Chief Privacy Officer, the Department of Homeland Security tasked the Committee -- is the tasking document associated with the paper when it's posted?

Mr. Ponemon: They both go on the side, don't they?

Ms. Landesberg: We can do it. We can do it, but it's not the normal practice. It's a public document.

Mr. Purcell: Well…

Ms. Landesberg: --.

Mr. Barquin: I believe that that sentence probably should be in the summary. You know, so it hits people right away, and then added in the, you know, in the recommendation. You know, that hour circulating was past way with doing this by the Chief Privacy Officer.

Mr. Purcell: Is there a need -- does the Committee express a need to review that specific language? Or is it sufficient to say that we will include an entry that indicates that this was the result of the direct tasking from the Chief Privacy

Officer?

Mr. Ponemon: Complete trust.

Mr. Purcell: Thank you. OK, Charles, I'll leave that one to you.

And John?

Mr. Sabo: Last comment. I would not bring this up. It's not a big deal, but I want to clarify something. Page four, policy enforcement -- this is a major header. This is one of the risk areas that was identified. As I read it, it really is focusing on security risk, that is, primarily data integrity and confidentiality. It doesn't really deal with risks associated with policy management generally with respect to the FIPPs.

So my suggestion, done of course structurally -- it looks like everything you're dealing with here are security risk areas, access control, auditing. Although auditing might be extensible to other aspects than security. So a question -- if this is intended to be primarily security policy enforcement, then I'd say that. But then I think there's a bit of a gap in terms of

policy enforcement generally with respect to data minimization and the other business associated with FIPPs.

So my way of dealing with that would be to say policy enforcement, and then use -- you know, just basically say with the ESB providing connectivity one or more services, all services providing guidance should ensure that policies associated with managing or enforcing FIPPs or requirements derived from the FIPPs shall be in place and then, use for example. For example, data transmitted over the ESB, which is more of a security.

So I guess it's a complicated point. But basically, are you intending it to be all policy manager or just security policy manager?

Mr. Barquin: No, clearly, clearly, it is intended primarily in privacy. But what if, you know, in that sentence that -- let me see, it's the first sentence that ends with data confidentiality is protected in ways appropriate, present a classification to ensure data confidentiality and

integrity. And there, add and -- I don't know whether compliance as the right word, but bringing it back to, let's say, compliance in quotes with the FIPPs.

Mr. Sabo: I think either, you know, slight expansion to suggest that appeal and/or the developers need to deal with policy management of the FIPPs generally and as appropriate or make this purely security, in which case, we have not done that. So I'd say you're approach would make sense if we just add that reference to the FIPPs.

Mr. Purcell: Ramon, can you give us the wording that you're -- you would -- you would intend there?

Mr. Barquin: At the end of that first sentence is…

Mr. Purcell: Yes.

Mr. Barquin: … so to ensure data confidentiality, I would say, comma, integrity and compliance with the FIPPs. And I would spell them out with the FIPPs, you know, the fair information practices. Yeah, and I don't know whether we would

need or want to go back to reported source.

Mr. Sabo: And then I would add the for example in front of encryption because the way it's written…

Mr. Barquin: For example, OK. Yeah.

Mr. Sabo: Encryption then is…

Mr. Barquin: Yeah, yeah, yeah.

Mr. Sabo: … like it's satisfying all that.

Mr. Barquin: Yeah.

Mr. Sabo: … and --. OK, thank you.

Mr. Alhadeff: Could I make a slightly different wording suggestion?

Mr. Purcell: Yes.

Mr. Alhadeff: At the -- because I think it should be at the top, not by the time you get to -- not by the time you get to confidentiality. So all services providing PII should be able to meet organizational policy and management requirements, period there. Policies ranging from those implementing FIPPs to those more detailed security policies related to -- and then you go ensuring data, et. cetera, et. cetera -- then covers that

broad range of policies and says the goal of this is top line policy, organizational policy enforcement and management that's related to this issue, not just FIPPs is thrown in as an afterthought after a litany of security requirements.

Mr. Sabo: Right.

Ms. McNabb: Yeah.

Mr. Purcell: Acceptable?

Mr. Sabo: Yeah.

Ms. McNabb: Yeah.

Mr. Purcell: Joe, can you give us that one more time, please?

Mr. Alhadeff: Sure. So once more with bravado, OK.

[laughter]

Mr. Alhadeff: So at -- start toward on the second line, all services providing PII…

Mr. Purcell: Yes.

Mr. Alhadeff: … or should be able to meet organizational policy and management requirements, period. Policies ranging from those implementing FIPPs to more detailed security policies requiring --

and then you have to change tense on the verbs -- ensuring data, et. cetera, et. cetera.

Ms. McNabb: Change the phrase here.

Mr. L. Hoffman: Can…

Ms. McNabb: Where is that going?

Mr. L. Hoffman: If Charles has that…

Ms. McNabb: That one.

Mr. L. Hoffman: … can you redact the entire paragraph?

Ms. McNabb: Policies.

Mr. Palmer: So this is just -- change, not the original accepted…

Ms. McNabb: So read it out again.

Mr. Barquin: This is the entire paragraph…

Ms. McNabb: Something's…

Mr. Barquin: … started, after the heading?

Mr. Alhadeff: So with the ESB providing connectivity to one or more services, potentially served in PII for requesting a service, comma, all services providing PII should be able to meet organizational policy and management requirements, period.

Mr. Purcell: And let me give you the amendment to fix the dangling part. At the beginning -- at the beginning of that sentence, it says policies covered should include those ranging from FIPPs implementation policies to more detailed security policies so that you have a complete sentence here.

Mr. Purcell: So that's the next sentence?

Mr. Alhadeff: Yeah.

Ms. McNabb: Yeah.

Mr. Alhadeff: Sorry, that was where the dangling portion was.

Ms. McNabb: Yeah.

Mr. Palmer: And it would continue, policies include those ranging from those implementing FIPPs to more detailed security policies requiring…

Ms. McNabb: Or such as data confidentiality integrity?

Mr. Palmer: Sure. That's good.

Mr. Alhadeff: I mean, essentially, you need to make the second sentence English.

Ms. McNabb: Yeah.

Mr. Alhadeff: But I think everyone can live with the gist now as being top line.

Ms. McNabb: And then is says this protection may require, for example, encryption? Is that what it is?

Mr. Alhadeff: Yeah.

Ms. McNabb: That's the way it goes?

Mr. Purcell: Right. For example, and the next sentence.

Ms. McNabb: Yeah.

Mr. Purcell: All right. I'm not terribly confident that I understand that whole sentence. So I am going to ask Charles to try one more time to read that sentence out.

Ms. McNabb: Two sentences.

Mr. Purcell: Two sentences now -- out prior to any approval vote.

Mr. Palmer: Make sure I got it.

Mr. Purcell: Yeah.

Mr. Palmer: With the ESB providing connectivity to one or more services potentially serving PII to a requesting service, comma, all

services providing PII should be able to meet organizational policy and management requirements, period. Policies include those ranging from those implementing FIPPs to more detailed security policies, such as those ensuring data confidentiality and integrity, period.

Mr. Purcell: There's a lot of those in there.

Ms. McNabb: A lot of those's.

Mr. Purcell: So may I suggest that we say these policies include those ranging from implementing fair information practices to security policies such as?

Mr. Alhadeff: And that -- yeah, OK, because that could also just be a semi-colon. That could also just be a semi-colon statement after the main statement. But at this point, I think we're wordsmithing to death.

[laughter]

Mr. Purcell: I agree.

Mr. Palmer: And the following sentence is this protection may require, for example, encryption for certain data, blah, blah?

Ms. McNabb: Yeah.

Mr. Purcell: OK, that was the easy one. So I -- I submit with the revisions that we've discussed here and are on the record the approval of -- I recommend the approval of the document with the revisions that we've discussed. Is there any further discussion? I put it to the Committee members for a raised hand vote, please? All those in favor of accepting the revised paper as presented? It appears to be unanimous.

Are there any dissenters to the acceptance to the paper there? I see none. The paper is accepted as approved. We will submit the finished copy to the Privacy Office through Martha Landesberg as soon as we're -- as soon as we're able. And everyone will receive a copy at that time. Thank you.

I turn our attention now to a paper that needs -- yes?

Mr. Harper: Would you like to many any comments about the attendance?

Mr. Purcell: I would like to make a comment

about attendance before we lose any further focus on attendance. A note for the record -- we have 100 percent attendance of the Committee members, something I am delighted with and -- and very pleased by.

Not only that, but I feel like we're in a -- we're in a groove here as far as being a -- being a group of people who not only are -- are recognizing people like Toby's professionalism, but also representing the professionalism of privacy and security data integrity in a way that, I tell you, it's very, very pleasing. And now you can go.

[laughter]

Ms. McNabb: Are you leaving?

Mr. Purcell: Jim's got to excuse himself for a -- for a moment. I had to get that in before we lost our 100 percent.

Ms. McNabb: Oh.

Mr. Purcell: The -- I'll ask the Committee's attention to be turned now to a report by the…

Ms. McNabb: Whoever we are.

Mr. Purcell: … data privacy and integrity --

no, you're the Subcommittee. What's your name?

Ms. McNabb: The other parts.

Mr. Purcell: What's your name?

Ms. McNabb: Yeah.

Mr. Purcell: We have, that's right.

Ms. McNabb: We're a combined.

Mr. Purcell: We put together a combined effort of two Subcommittees in order to produce, not only a response to the tasking on the elements of redress, effective redress, but also the requirements in terms of communicating and educating individuals about that redress program.

So I'll ask Joanne McNabb to give us a summary.

Ms. McNabb: Yeah, I will begin, and then my co-combined task force chair on this project will -- David -- will end.

This was, indeed, as we say in here -- well, we don't exactly say it. This is in line with the White House memorandum about openness and transparency and public participation, collaboration. And we were asked by Mary Ellen to

provide the Department some guidance in the form of -- of identifying the elements of effective redress and strategies for communicating and educating people about redress procedures, which is what we have done here.

We looked -- we've approached this first as redress in a basic way that would be applicable to any kind of organization that makes decisions that -- that affect people. And then we moved on to identify some specific issues that come up for Homeland Security. So our initial definition and the elements that we identified are applicable beyond Homeland Security. And I'm going to speak to that part of it.

The definition is from the dictionary. And it's basically redress is to set right, rectify or remedy a wrong. We point out that in this -- that redress can be addressing simple errors, simple kinds of wrongs or can, in fact, be aimed at very significant liberty interests. And there's a whole range. These principles in general apply to the whole range.

The elements that we identified are one, two, three, four, five. Are there five? No? There's more. But we'll add them up.

Clear ownership and accountability from the redress seeker's perspective -- it isn't acceptable to say it's his fault, go there, it's their fault, go there. It has to be clear who's in charge of the program and that there's a single source that can be consulted to seek redress.

The redress procedures must be visible to people. A secret process is not very helpful. It must be easy to use. We note that redress seekers are often distressed and the -- a complicated process is particularly challenging in that situation. Obviously, it needs to be timely.

And importantly, it -- an effective redress program must actually right the wrong, not just identify that wrong has been committed and continue to commit it. It should have a right of appeal, if the original adjudication isn't satisfactory.

And importantly, there -- these must be

more than just policies, but an entire infrastructure to make it possible for the redress program to actually work.

We then identify the FIPPs support for privacy redress in particular. The entire intent of FIPPs is, in fact, to give people control over their personal information. And that's what is being redressed in privacy redress, an apparent lack of control or inability to control.

And then on public education, the -- one of the points that we emphasize is that information about the reader's process should be available, not just on websites or over telephones, but also on -- at the sites where wrongs are experienced.

And since among the redress seekers in many cases would be people whose native language or who are foreign nationals, their group's native language is not English, that basic information should be available in multiple languages and that the information should be provided not just in the form of FAQ's and standard answers, but also it should be a learning process, where as new issues

are raised and new complaints come through the information available is updated and improved.

So that's the general information in this paper on redress. And now, specific issues facing the Department.

Mr. D. Hoffman: So we wanted to then in the second part of the paper do an analysis of the particular difficulties that DHS might have fully effectualizing those elements to create a fully impartial redress mechanism. To do that, well, the first thing we wanted to look at was the -- some of the existing redress mechanisms that either exist within DHS or exist within the Federal Government and DHS is -- plays a portion of – we looked at the Privacy Act.

We looked at the Traveler Redress Inquiry Program, TRIP. We looked at the Computer Fraud and Abuse Act. And we looked at the Freedom of Information Act and the processes under those either pieces of legislation and their programs to provide redress.

And by analyzing those then the paper

recognizes that there are three different categories of redress mechanisms. And then there can be mixes within mechanisms of these three. Those three categories are administrative redress. So that there's actually an administrative process within the particular agency or component or how to provide that redress.

There's Privacy Office redress. So issues that come directly to the Privacy Office and the Privacy Office acts to create redress for individuals. And then there's opportunities for judicial redress. So going to the courts to actually get redress.

We then looked at what challenges there are for DHS for those existing mechanisms, specifically calling out three particular challenges: one, the challenge of when you're talking about a situation providing redress in issues that have to do with the provision of national security. There's going to be situations that arise, where it would be inappropriate to provide full information to the individual who has

been impacted of all the information that relates to the particular issue.

A second challenge was the difficulty or impracticality of taking advantage of some of the judicial redress mechanisms. So with difficulty, we're talking about legal difficulties particularly around standing. From impracticality, we're talking about the situation of really does an individual really have the knowledge and the capacity to bring this kind of a claim. While it might be possible that they would do that, do we think that it's probable that most people are going to feel that that's an effective mechanism for them to take advantage of?

And then the third concern that the paper notes is the concept of the fox guarding the hen house. When is it appropriate to have the individuals who are actually in the organization that was originally processing the data or making the determination being the individuals that are making the determination about the redress?

There's arguments to be made that that's a

fundamental component of an effective redress system, because you need the people who really understand the particular processes that are in place and what has happened to understand how we address it. But there's also arguments to be made that you need to have to some way to appeal outside of that body to be able to get to somebody who would be more impartial in the way that they would look at the final determination.

So with all of that analysis then, the paper makes a series of recommendations. First recommendation is to assign accountability for the privacy redress process to a single owner with responsibility for developing and managing policies and processes that make the program accessible, understandable and fair.

Second recommendation is provide information to the public that explains redress seekers' rights, the process for complaining or seeking redress, a general timeline for the process and the privacy policy regarding the personal information used in the process.

The third recommendation is provide descriptive information on the process in plain language in an easy to read format in languages appropriate for the people seeking redress at points of contact with individuals and organization Web sites and in other available venues.

Fourth, develop and deploy a training program that educates employees, contractors, vendors and others as appropriate about the redress policies, procedures, standards and access points. Train staff handling redress cases to be patient, helpful, and sensitive to cultural or linguistic differences.

Fifth, ensure the corrections or annotations are propagated throughout all primary and secondary systems to prevent the same information for producing an adverse impact in the future.

Next, set service standards for logging redress complaints and providing timely responses and promote transparency and accountability by including the standards in publicly available

documents, including the complaint intake forms.

Next, develop administrative and technical support for the redress process to integrate it into the regular workings of the organization. Then establish, administer, and monitor on appeals process designed for transparency and fairness.

And then for the last recommendation that we make, we actually have a change to the document. There were some mistakes made in the final recommendation. The new language should read, "develop and implement an effective redress appeals process that provides individuals with confidence that the ultimate reviewer is appropriately impartial and separate from the entity that is the subject of the appeal."

So to the chair, that is our report and our recommendations.

Mr. Purcell: Excellent, thank you.

All right, Renard?

Mr. Francois: I just want to say that I thought everybody did an excellent job on this. I have a few comments. And so, work schedules -- I

was unable to kind of forward these to you all in advance to give you a heads up.

It's not that bad, I don't think.

[laughter]

But there -- really my comments focus on three areas. And the first one is -- and the redress is on page two under the subtitle of "clear owner and accountability." When I read that section, it really speaks more towards clear ownership. And there's not much on accountability. And maybe it's a perspective issue. But my from my perspective, accountability means, OK, you have a process owner. To whom is that process owner accountable? And what are the expectations to which that process owner will be held?

And I think it's important for -- because as you say in the first page, this is going to be applied to a lot of organizations, not just the government. And I think having, quote, unquote, "that one throat to choke," in terms of who is responsible…

Ms. McNabb: I like that term.

Mr. Francois: … what are they going to be doing and, you know, what you have here is learn lessons, make reports. But I think you have to have some sort of language that says you've got to be accountable for making these changes and implementing the redress and taking steps to implement the lessons that you've learned. So that's the first.

And I've suggested some language that will hopefully be kind of painless to include and hopefully gets at that. But it's policymakers and the process owner should develop periodic actionable expectations for which the process owner will be held accountable.

Ms. McNabb: Renard, I'm just -- I looked over at the recommendations for it. It says set service standards for, you know, that one third up?

Mr. Francois: Yes.

Ms. McNabb: How about if it said something like the owner should be accountable for the policies -- for implementing the policies, the redress policy then service standards?

Mr. Francois: OK. I think that's the sufficient.

Ms. McNabb: For any -- form anything, redress policies and service standard.

Mr. Francois: The second is just a suggestion on page three under the bullet point effectiveness, righting the wrongs. And my suggestion would be to just strike the first sentence, and then move the last sentence to become the first one.

And there are two reasons why. The first is if you look at all of the language in the subtitles, they're very strong in terms of redress should, programs should, process should. And then, we kind of get to this point and we lose…

Ms. McNabb: Or at least…

Mr. Francois: … that, we lose that language. And then the second is I think that's the last sentence -- what's currently the sentence is really the most powerful point of that section. And it -- you kind of buried the lead on it.

Ms. McNabb: I like that.

Mr. Francois: And so, I would suggest

switching that.

And the third area -- and this might be just my understanding. But I found that on page four, the redress challenges -- I found that to be a very confusing read. Because I go through the first paragraph. And I think that this is about the benefits of having better privacy officials and the elements of an impartial redress program at DHS.

But then later on, I just get lost a little bit. And David's summary -- actually, my suggestion would be to just incorporate David's summary, just get -- because it really clarified what the approach was and what you were looking at. And I didn't get that from looking at the first paragraph and then the subsequent paragraphs in support of that -- of this principle.

So -- and then I just had a couple of questions about the Computer Fraud and Abuse Act. My experience with it has not been that it's been used in this instance, because it sounds like what the intent -- what the use is suggesting in this paper is an individual can sue either an employee

acting -- an employee of DHS acting outside of the scope of their responsibility for, you know, improperly accessing personal data.

From my vantage point, being an in-house counsel, I've seen companies use it against individuals in a company not necessarily in the government for improperly accessing information outside of the scope of their authority.

Mr. D. Hoffman: It could be used either way.

Mr. Francois: OK. And I think maybe clarifying that -- because you know, I read this and first thing I put down was really? And so, maybe it's just a clarifying sentence somewhere that illustrates that.

And so, to go back to the first paragraph, maybe the suggestion would be for me to give a little bit -- to tie it together in the way that David so eloquently did would be to keep the -- I'll read the part of the last sentence that I would keep as -- complete independence, however, would deprive redress seekers of the benefits that currently -- that exist within the current legislative,

regulatory and judicial framework.

All of the examples that you cite in the subsequent paragraphs and even in your discussions made it go to that legislative, regulatory and traditional framework.

Mr. D. Hoffman: We're going to -- I don't want to be difficult, but I'm probably going to be on this.

Mr. Francois: OK.

Mr. D. Hoffman: I'm not seeing how that makes this more clear. I think the point that this is trying to make is we have -- you have individuals that run these organizations. You have privacy officials embedded within those organizations. And you want to make sure that they're playing a part in the redress mechanism.

Other people have asserted that redress mechanisms should be completely outside the components. This is making a point -- and I thought it was making the point fairly clearly -- that you actually -- at least at some point in that redress mechanism, there is benefit to be gained from those

privacy officials, similar to the way we do this in the private sector, having privacy officials that -- embedded within that organization so they neatly understand the process. And so, I'm reticent to go and broaden it in the way that you're recommending.

Mr. Francois: Yeah. And I don't -- from the text, I don't draw the same conclusion that you have articulated.

Mr. D. Hoffman: So let me read the text. "Complete independence, however, would deprive redress seekers of the benefits of privacy officials embedded within the organizations that are processing personal data and the many elements of impartial redress that are currently in place for DHS."

Mr. Francois: I get that. And then, the first paragraph after that, that starts with legislative and regulatory, I think that's fine, given the first paragraph that you read to me.

But then, there's the reference to the paragraph that starts with the Computer Fraud and Abuse Act. And I lose track of what that has to do

with the embedded privacy officials? For…

Mr. D. Hoffman: OK, now I'm understanding. So it's…

Mr. Francois: And so…

Mr. D. Hoffman: … it's not an issue with the language…

Mr. Francois: No.

Mr. D. Hoffman: … around the embedded --. It's the…

Mr. Francois: No.

Mr. D. Hoffman: … an issue with the flow…

Mr. Francois: Right.

Mr. D. Hoffman: OK, so let me take a look.

Mr. Francois: I get the point of what you're trying to make. And I think it makes sense, but I just -- I get tripped on here thinking, OK, that paragraph is about an individual…

Mr. D. Hoffman: So…

Mr. Francois: … suing an individual, but what about the embedded privacy officer?

Mr. D. Hoffman: So let me make a proposal then, to deal with that, because you're actually

pointing out something where we had some other language, and we cut something. And I think it's a really good point that doesn't flow particularly well now.

If we did an introductory sentence before the Computer Fraud and Abuse Act…

Ms. McNabb: Or before the legislative and regulatory landscape.

Mr. Francois: Yeah.

Ms. McNabb: After the first paragraph.

Mr. Francois: Yes.

Mr. D. Hoffman: Yeah --. Yes, I think that's the right place, where we say…

Ms. McNabb: Now we're going to talk about…

Mr. D. Hoffman: So we have subject titles underneath. And if we add it and so we've got challenges due to impartiality, challenges due to transparency -- if we included a subject title between the first and the second paragraph that said something like existing redress examples.

Ms. McNabb: Or existing legal redress.

Ms. Anton: Well, then you've got regulatory…

Mr. D. Hoffman: Right.

Ms. Anton: You've got…

Ms. McNabb: Yeah.

Ms. Anton: … legislative, regulatory and legal.

Mr. Francois: Right.

Mr. D. Hoffman: That's why it previous should just be existing redress examples.

Ms. McNabb: Or mechanisms.

Mr. D. Hoffman: Or mechanisms.

Mr. Alhadeff: Since you call them mechanisms in the paragraph before you get to --.

Ms. McNabb: Yeah. That's --.

Mr. D. Hoffman: Would that take you there?

Mr. Palmer: That works.

Mr. D. Hoffman: OK.

Ms. McNabb: … 15, redress. Got it.

Mr. Purcell: Anything else?

Mr. D. Hoffman: That's it.

Ms. Anton: I have – I do have a comment.

Mr. D. Hoffman: That was very little damage.

Ms. Anton: I actually do have a comment.

This section is called redress challenges. So if we put in a new subtitle for the -- a new subsection called redress -- existing redress mechanisms, then that ruins the flow of the subset -- of the section where the subsections are…

Ms. McNabb: How about if we call it limits of existing redress? Because that's the point that's being made isn't it?

Mr. D. Hoffman: Before we go there, I want to understand why that ruins the flow? Because I'm not…

Ms. Anton: Because this section's called redress challenges.

Mr. D. Hoffman: Yeah.

Ms. Anton: Which means any subsection should be about challenges. And the title that we placed -- new subtitle that suggested…

Mr. D. Hoffman: Well…

Ms. Anton: … is a positive thing. It's existing redress mechanisms. It's not challenges to redress mechanisms.

Mr. D. Hoffman: Maybe, but it's not just

redress challenges. It's redress challenges for the Department of Homeland Security. So this first subset is to lay out what are the mechanisms that already apply to the Department of Homeland Security.

Mr. Sabo: I think Annie's point, though, is -- I mean, why not just say redress in the Department of Homeland Security, make it much -- statement?

Ms. Anton: Yeah.

Mr. D. Hoffman: That's -- that would be fine.

Ms. Anton: Yeah.

Mr. Sabo: Yeah.

Mr. D. Hoffman: That makes sense.

Ms. McNabb: Redress in or redress for?

Ms. Anton: Probably in.

Mr. Sabo: In.

Mr. D. Hoffman: In?

Mr. Sabo: No, that's good. All redress…

Ms. McNabb: Yeah. So the whole section area, redress in the Department of Homeland Security? Good. Good.

Mr. D. Hoffman: And that better captures what

we were trying to do with that entire sentence. No, that's a good point.

Ms. McNabb: That's good.

Mr. Purcell: Are there other comments? Yes?

Mr. Alhadeff: I have no problem with Renard's moving the last sentence -- I'm sorry, page three -- to support the concept of moving the last sentence to the first sentence. But a couple of edits that have to have that sentence to make more sense -- the first one is the result of redress should be certainty, because we're now at the end…

Ms. McNabb: Yes, yes.

Mr. Alhadeff: So and then the other question I have trouble understanding what we're saying is at the end of that sentence, we said individuals should not be repeatedly be affected negatively by an error or by information that has been corrected.

Male Speaker 3: --.

Mr. Alhadeff: Yeah, I would think when the information is corrected, you're not negatively affected.

Ms. McNabb: Actually, you are. And that's

one of the problems. It's corrected in one place, but it's not corrected in every place.

Mr. Alhadeff: Yeah, but that's -- but you're saying…

Mr. Purcell: Right.

Mr. Alhadeff: … the information that is corrected is the problem, not its propagation to other places is the problem. So the way it reads, it sounds like when you correct information, you still have a problem. You only have the problem when you correct information and it is not propagated across sites.

Mr. Purcell: Right.

Mr. Alhadeff: So something needs to be there to make that sentence make more sense when it's read.

Ms. McNabb: It makes sense at the end, because it's prepared for by the two sentences before it.

Mr. Alhadeff: I read the whole paragraph, and I think, you know, we who naval gaze on this topic…

Ms. McNabb: Yes.

Mr. Alhadeff: … for a long time understand exactly what the problem is.

Ms. McNabb: How about this? How about if we take -- if we make the first sentence the result of redress should be certainty, period? Then leave the rest of it, starting with "it may not be enough" and get rid of however -- it may not be enough simply to correct the da, da, da. And then the last part reads "individuals should not repeatedly be affected negatively."

Mr. Purcell: Well, I -- the -- I'm with Joe. I -- the issue remains that if you say the sentence "individuals should not be repeatedly be affected negatively by an error or by information that has been corrected…

Mr. Alhadeff: You could fix that by saying incomplete transmission or incomplete dissemination of information that has been corrected.

Mr. Purcell: But not fully published.

Mr. Alhadeff: Yeah.

Ms. McNabb: Uh-huh, uh-huh.

Mr. Alhadeff: Then so I think I can take it

on faith that we can allow that wordsmithing…

Ms. McNabb: That's not…

Mr. Alhadeff: … to happen? The next topic, the right of appeal -- when you first read it, I mean, you understand what it means. But the whole concept says organizations should have an appeals process. And it sounds like it's an appeals process for the organization. Just a clarification -- it might say -- it might read better to say "organizations should provide an appeals process".

I was a little unclear as to what the last sentence of the next topic meant. "Those charged with handling redress requests should approach their work as case workers." Does that mean they should be sensitive, they should handle it on an individualized basis?

Mr. Herath: Yes.

Mr. Alhadeff: I don't know that there's a general national short hand for what a case worker is and how they handle their job.

Ms. McNabb: Yeah.

Mr. Herath: Yeah, Joe, I believe that that

would be a good clarification.

Mr. Alhadeff: OK.

Ms. McNabb: I think the intent, this version of John's language, the intent was they should be advocates for the people seeing redress. They should be seeking to satisfy, you know, to do their best for the people seeking redress as opposed to…

Mr. Alhadeff: I think that would be a useful clarification.

Ms. McNabb: … inappropriate attitude.

Mr. Alhadeff: Yeah. Sometimes that may happen even with a case worker.

Ms. McNabb: Yes, you're right. As advocates, how about that?

Mr. Alhadeff: OK.

Mr. Purcell: Redress seeker?

Ms. McNabb: For redress seeker, yeah, for redress seekers?

Mr. L. Hoffman: Joanne, can I comment on that?

Ms. McNabb: Uh-huh.

Mr. L. Hoffman: I'm not sure we want to run down that slippery slope.

Mr. Purcell: Yes.

Mr. L. Hoffman: I'm not sure we want to run down that slippery slope so fast. Even though I am on this Committee, we didn't have the advocacy word in there until just a second ago as proposed. And I -- I like the idea of the case approach. That's just fine. But I'm more for them impartially looking at things independently or whatever David's word was to get the, you know, the…

Ms. McNabb: Uh-huh.

Mr. L. Hoffman: … separation. But advocate…

Ms. McNabb: Uh-huh.

Mr. L. Hoffman: … implies that any bogus claim, they're still going to be the advocate boy and I want to avoid that.

Mr. Alhadeff: I mean, we could use something like "should assist to redress requestors in the -- in the proper functioning of the system" or something, so that it indicates that they have a role in helping smooth the system out, but not necessarily that they are an advocate one way or another, but that they are a resource.

Mr. L. Hoffman: You know, all this doesn't have to do -- this last sentence, those charged with handling redress requests, doesn't really have to do with the integrated infrastructure.

Mr. Alhadeff: Yeah.

Ms. McNabb: Uh-huh.

Mr. L. Hoffman: So I'm wondering if it's important enough to even leave in, but…

Mr. Purcell: Retain the sentence? Perhaps delete it?

Mr. L. Hoffman: Yeah.

Mr. Alhadeff: That works, too.

Mr. Purcell: Anybody concerned about deleting that sentence entirely?

Mr. Herath: No, well, actually, I am. I found this pretty important. And actually, Joe's first language that didn't deal with advocacy and dealt with sensitivity and -- was more appropriate. But do you remember what -- literally, it was a clause that would have dangled…

Mr. Alhadeff: I said, you know, would it mean that they would deal with cases in a sensitive

manner and on an individualized basis?

Mr. Herath: Yeah.

Ms. Callahan: You know, we do have something like this…

Mr. Herath: I think that's good, yeah.

Ms. Callahan: … in the recommendations some…

Mr. Purcell: I think it's in the recommendations.

Ms. Callahan: Yeah.

Mr. Purcell: I mean, under the training and…

Ms. Callahan: Yeah.

Mr. Purcell: … and education.

Mr. Herath: You help him navigate it.

Ms. Callahan: Where you -- yeah.

Mr. Purcell: Under the fourth bullet -- develop and deploy a training program that educates employee contractors, vendors and others as appropriate about the redress policies, procedures, standards and access points. Train staff handling redress cases to be patient, helpful and sensitive to cultural and linguistic differences.

If we delete it from the body, the

recommendation remains and stands on its own, I would think. Is that appropriate then to delete it from the body?

Ms. McNabb: It's OK with me.

Mr. Purcell: Kirk, you OK with that?

Mr. Herath: Why not just add it back into the body and it’s two places? It’s only a few more pieces of --.

Ms. McNabb: And mirror the languages one to the other?

Mr. Herath: Yeah, and the language could be mirrored. And then it’s -- the fact that it’s repeated in the recommendations is irrelevant -- it's -- yes, that works.

Ms. McNabb: That doesn’t make sense under integrated infrastructure.

Mr. Purcell: Well, actually, it does in the sense that you haven’t talked about training in any of the other parts.

Ms. McNabb: Uh-huh.

Mr. Purcell: In those seven elements.

Ms. McNabb: Yeah, it’s kind of an ease of use

in a way. It's not stated, but that would -- to my mind, that's where it would go.

Mr. Purcell: Wouldn't educating the providers of the service -- the training?

Ms. McNabb: Oh, yeah, that's part of the infrastructure, yes.

Mr. Purcell: Can you integrate it into the infrastructure?

Ms. McNabb: Yes.

Mr. Purcell: So I -- may suggest that you clip the…

Ms. McNabb: Yeah.

Mr. Purcell: … copy, the trained staff handling under point four of your recommendations? Appropriately smith it and replace…

Ms. McNabb: Uh-huh.

Mr. Purcell: … the last sentence of that…

Mr. Herath: Yeah, that's fine.

Mr. Purcell: … paragraph with that?

Ms. McNabb: That works.

Mr. Herath: Yeah.

Mr. Alhadeff: Next topic is -- I'm not a

footnote expert, but footnote three seems a little bit non-standard.

Ms. McNabb: Oh, yeah.

[laughter]

Ms. McNabb: I went back and fixed that one. So my -- I had a question. Nobody ever responded to that question mark. What's the matter with all you guys?

What -- because of the location in here, I didn't think -- it doesn't seem appropriate to put -- to cite it to the DHS statement of FIPPs because this is before we get into -- so I'll do the OECD thing. Yes, that can be fixed.

Mr. Alhadeff: OK.

Ms. Sotto: Another alternative…

Ms. McNabb: Yeah.

Ms. Sotto: … Joanne, is to use the most recent articulation by the FTC, which I think is 80 -- was 98.

Ms. McNabb: But that's FIPPs light.

Mr. Alhadeff: They're not internationally recognized.

Ms. McNabb: Yeah. And it's like notice of choice and blah, blah, blah. Yeah.

Mr. Purcell: We can…

Ms. McNabb: And you're essentially the same at OECD.

Mr. Alhadeff: The last thing I wanted to highlight is in the public education portion with the sense is, additionally the right to be heard. And I think the right to be heard is critically important, but I don't really see it reflected specifically in the effective elements of a redress program. And I think it probably would be useful to echo it there.

And one of the things I noticed when you look at the clear ownership and accountability, the third sentence in that, which starts "individuals should not be expected to determine which component," -- is really not clear ownership or accountability. That's a person's ability to access a service.

And there might almost be a rationale for having a right to be heard as a topic within these

elements that kind of expands a little on that one sentence, because there's a difference between what is clear ownership and accountability in that sentence, which really goes more to the concept of there is not wrong door for the person to go to. They can't figure out the infrastructure of DHS.

They have to be able to complain and have the owners allocate that complaint to the right place, because they can't figure out which sub-component may be responsible, which is a different concept that's kind of chained the ability of -- it might fit under visibility. And maybe using the word "right to be heard" under visibility would be a solution without having to create a new topic.

Ms. McNabb: How about his? How about if that sentence that you just cited in the fair ownership and accountability starts with "individuals have a right to be heard; semicolon, they should not be affected"?

The reason for having the -- figure out which component is that is the rationale for why there needs to be clear ownership.

Mr. Alhadeff: Right, but the -- but the sentence then in that -- for me, this sentence is still phrased as a sentence directed to the individual, not to the owners. What the -- a version of that sentence directed to the owners would be owners must have systems that allow for individuals too, because then you're in a clear ownership section. It just doesn't…

Mr. Sabo: Hey, Joe?

Mr. Alhadeff: Yeah?

Mr. Sabo: Why not combine it with ease of use?

Mr. Alhadeff: Oh, that would actually be better, yeah.

Mr. Sabo: Right to be heard and ease of use. And then just have an opening sentence.

Mr. Alhadeff: Yeah, that's fine.

Mr. Sabo: And then, the transition is in addition -- or you know, then you can move into the importance. You can start with an opening…

Ms. McNabb: Yeah, OK.

Mr. Purcell: So John…

Ms. McNabb: Individuals have a right to be heard is the first sentence of ease of use. Nothing changes in clear ownership and accountability. Just that goes into ease of use, right?

Mr. Purcell: Sufficient?

Mr. Sabo: Marginally.

Mr. Alhadeff: Marginally. And it's not worth arguing about.

Ms. McNabb: Well, no go on. What were you?

Mr. Alhadeff: So I just don't think that individual sentence is written to say…

Ms. McNabb: This one?

Mr. Alhadeff: … yeah, I don't think it's written to say that it's an obligation on owners to create. It says this is a right of individuals. But I don't think it's directly linked to the obligation on the owner.

Mr. Purcell: May I make a suggestion, Joanne?

Ms. McNabb: Yes.

Mr. Purcell: Move the "individuals should not be expected" sentence from clear ownership down to the first sentence of ease of use section so that

that section would then say the individuals should not be expected to determine da, da, da, da. It is -- and then following sentence, "important for all organizations…"

Ms. McNabb: So that would come after "individuals have a right…

Mr. Purcell: To provide clients…

Ms. McNabb: … to be heard?"

Mr. Purcell: Right.

Ms. McNabb: They should not be expected to ba-da, ba-da, ba-da?

Mr. Purcell: Correct.

Ms. McNabb: OK.

Mr. Purcell: And then, in replace -- since you've clipped that sentence out and pasted it somewhere else, in the clear ownership, following Joe's thinking, it would be appropriate, it would seem, that to make an entry there, saying that organizations should, and Joe help me out with that…

Ms. McNabb: Yeah.

Mr. Purcell: … wording that would like in there. But it's about the organization owning the

process, as opposed to individuals accessing the process.

Mr. Alhadeff: That's right, but it's the question of organizational responsibility should account for the ability of individuals to complain in an effective manner without determining the component responsible.

Ms. McNabb: So after where possible the ownership being the same public facing entity, comma, otherwise -- like where it isn't possible…

Mr. Alhadeff: Yeah.

Ms. McNabb: … how you said that?

Mr. Alhadeff: Or get -- I wish I had written it down when I said it. Organizations should be responsible…

Ms. McNabb: Or organizations should be able to…

Mr. Alhadeff: … receive.

Ms. McNabb: … receive and address…

Mr. Alhadeff: Yeah.

Ms. McNabb: … redress requests.

Mr. Alhadeff: How about…

Ms. McNabb: At any place…

Mr. Alhadeff: … cross components?

Ms. McNabb: … no, you don't want to say any place.

Mr. Alhadeff: Receive and refer to the proper agent.

Ms. McNabb: Yeah.

Mr. Alhadeff: Proper.

Ms. McNabb: It's the referral part we're trying to get away from.

Ms. Anton: Be capable?

Ms. McNabb: Yeah, of what? The…

Mr. L. Hoffman: Even if the individuals cannot, where you say -- where you're dealing with that…

Ms. McNabb: It can't be the public facing entity. So here I am, but it's…

Mr. L. Hoffman: It can't be organizations should nevertheless be able to properly process the requests with no more burden on the individual. So the onus is on them, the organization, to get it to the right place.

Mr. Purcell: Are you able to…

Ms. McNabb: Because -- I mean, the idea is -- what we're trying to say the negative is go somewhere else, it's not us. And yet, you're the one who just told me I can't whatever.

Mr. Beales: How about this? Go back to what you had. Forget the changes you just made…

Ms. McNabb: Uh-huh.

Mr. Beales: … in the -- or that were just suggested.

Ms. McNabb: Uh-huh.

Mr. Beales: And instead of individuals should not be expected…

Ms. McNabb: Uh-huh.

Mr. Beales: … start that sentence by saying "organizations should design a process that does not require individuals…

Ms. McNabb: Yeah.

Mr. Beales: … to determine which component of the organization."

Mr. Purcell: Good.

Ms. McNabb: That's good.

Mr. Beales: And then leave it the way you had it.

Ms. McNabb: That's good.

Mr. Purcell: Thank you.

Ms. McNabb: Whew.

Mr. Purcell: Are there other comments, revisions, or inputs to this?

Mr. Barquin: I just have one comment.

Mr. Purcell: Ramon?

Mr. Barquin: It's just a comment. And I don't in any way mean for it to, you know, imply anything, you know. I just wanted to know the one -- - within DHS, the one very, very specific organization focused on redress or hopefully prevention of redress is the ombudsman's office. And has specifically with USCIS. And I was just wondering whether there was anything there that you had looked at, that was useful to relative to that paper.

Mr. Palmer: Do you have some --?

Ms. McNabb: Yeah.

Mr. Palmer: It's a question.

Ms. McNabb: No, we didn't look at USCIS. We start -- we actually made it -- a decision early on, other than looking very closely at TRIP and the OIG report -- that what we were asked for was the elements of effective redress, not an evaluation of DHS redress process.

Mr. Barquin: No, I understand. But again, the ombudsman office is not a part of USCIS. It's within the law. And it was created sort of as a way to ensure that the immigration process…

Ms. McNabb: So that could meet some of these…

Mr. Barquin: … and just a question with…

Ms. McNabb: … criteria.

Mr. Barquin: … whether you looked at some of that stuff, because it might be useful. But I think that's above and beyond for the future.

Mr. Purcell: Might be a good follow up after -- thank you. Any other comments?

Mr. Pattinson: Richard?

Mr. Purcell: Neville?

Mr. Pattinson: Where line up, for page three, back on page three, timeliness -- just to comment on

the second sentence of the section an organization must provide -- I would recommend here must provide closure for each redress submission received in a timely manner.

Ms. McNabb: Yes. That's good.

Mr. Purcell: To conclude?

Ms. McNabb: That's good. Each redress…

Mr. Pattinson: … submission received in a timely manner.

Ms. McNabb: OK. -- in a timely -- received.

Mr. Pattinson: OK.

Ms. McNabb: I like that.

Male Speaker 4: Richard?

Mr. Purcell: Yes.

Male Speaker 4: The only comment is the resymmetry that we actually have the tasking order - - that same sentence…

Mr. Purcell: Right.

Male Speaker 4: … we can basically…

Mr. Purcell: Agreed. Agreed.

Ms. McNabb: Yeah, that'll fit in very nicely. We're almost there.

Mr. Purcell: We've had a lot of revisions. Is the Committee comfortable with the understanding of what the revisions' affect on the document will be? Given that, and requesting that Joanne rewrite the document to include those revisions, I would ask the Committee now to vote for the approval of the document.

Are they -- we'll use in the same procedure. All those in favor of approving the document with these revisions, please raise your hands. Are any opposed to the approval of the document? There are none. So by unanimous vote, we have approved that.

The Committee then has voted to adopt that report. Again, I will ask Martha Landesberg to take the necessary steps to formally submit the report to Secretary Napolitano and our Chief Privacy Officer Mary Ellen Callahan and to see that it is also posted to the Committee's Web page.

Thank you very much to the authors, the Subcommittees, all the Committee members' involvement both in the creation and the necessary

revisions. They do improve the product. And I'm quite happy with the -- with these results.

We've come to the portion of our meeting where we typically take comments from the public. We have received no requests to address the Committee. I think we've worn out our welcome for the -- if -- if we nitpick our own selves this much, what would we do to a member of the public if they addressed us?

So forbearing that, that puts us well ahead of schedule, I'll say, which is terrific. I would like to take an opportunity as I promised earlier to allow the Committee to address Mary Ellen Callahan. That's right.

There were a few comments that we wanted to make. We have a few moments. And I would like to -- to open the opportunity for the Committee to address any questions to our fearless leader.

Joe, starting off?

Mr. Alhadeff: Yeah, this was -- this was a little kind of going back to thinking about the soft stuff is the hard stuff. And…

Ms. McNabb: I like that phrase.

Mr. Alhadeff: Yeah, and in my experience, when I did some work on some committees with state, justice officials and state law enforcement officials, they had been used to, for the most part, working in criminal situations, where they were very, very protective of the information related to witnesses and the information related to victims. And the privacy paradigm was really set up in that fashion.

As we start having systems of DHS that are more broadly accessed, especially outside of the federal zone now, I was wondering -- I know we discussed in the grand situation the ability to urge and encourage. But I was wondering is there a way to actually either require or find a way to disseminate some of the very useful tools that the Privacy Office has done to better educate some of those folks who may have come from a very narrow criminal experience into some of the broader requirements almost like in many ways companies sometimes have a set of education tools you have to

go through before you can access the system.

And I was wondering if there's anything that the Privacy Office might be able to do to suggest that, so that there's a broader exposure to concepts than perhaps exist in some of the organizations, which have to attach to this information now for completely legitimate reasons, but who may not understand the consequences of how it needs to be treated, because of their previous experience.

Ms. Callahan: And I think you're exactly right, Joe. I think though that education is only the first step of that conversation. As I mentioned, together with CRCL, my office is working on pushing out more privacy and civil liberties training through this train the trainer program that will take place in the four regional fusion center conferences.

We are then having a follow-up, to make sure that indeed the training has been provided and to do an assessment on whether or not the training has essentially been incorporated or been

internalized within it. And I think that that's, again, a threshold beginning part of the conversation, whether or not the fusion center accesses DHS information. I think it's just what's necessary for privacy protections in the fusion center context to have them understand it.

And I will say in my conversations with the fusion center directors, they were very open to this, to have a continuing dialogue, to have a continuing observation because they understand that it's a least common denominator phenomenon at the fusion center. So if there's a privacy problem in one fusion center, it affects all 72.

But as I said, the education element, I think, is just the first element of it. We do have actually pretty exhaustive material provided on a Web site that DOJ hosts for the fusion centers, that is very good. And it has a lot of these elements in it. And that will be discussed in the train the trainer program and will be pushed out. And we'll we see how it has been useful.

In addition, I've had conversations in my

office about, you know, whether to do reviews of the fusion center or alternatively, work with the fusion center to do their own reviews in terms of how are privacy and civil liberties protections incorporated with information, not just the law enforcement information. But I agree.

Mr. Alhadeff: Just a quick follow-up, because it's less of a concern of those folks who are in the fusion center than those state organizations who might be accessing the information through the fusion center. And so my question is - is there a way to get that educational component down that one more level to who might be the person who's the ultimate user of the information, not the organization that is actually maybe helping to facilitate the query or evaluate the process?

And because I think the folks who go into the fusion centers do get that training.

Ms. Callahan: Uh-huh.

Mr. Alhadeff: The folks who may be touching the information that are just within a state of organization, may not have that awareness. And

that's why I was just saying the propagation of the tools may be the first step there.

Ms. Callahan: I do not believe that somebody in a state organization can access DHS material unless it's in an authorized setting. And I think that we have training -- required training associated with that.

But the bulk of -- if there were -- if there were DHS systems that were being accessed, the bulk of that would be done at a fusion center rather than in a state agency outside of the center. But I think that there is required training to access any of the DHS systems. But we'll double check.

Ms. McNabb: And then there's other data suppliers supplying data to the fusion centers. And they're subject -- at the state level, they're subject to their state laws already, some of which…

Mr. Purcell: Yeah.

Ms. McNabb: … in California they are.

Mr. Purcell: In whatever condition they may be.

Ms. McNabb: Yeah.

Mr. Purcell: Fine. Lance?

Mr. L. Hoffman: OK, Mary Ellen, I ask if you could expand on your remarks earlier this morning on the grant guidance?

Ms. Callahan: Uh-huh.

Mr. L. Hoffman: Because it's been a vexing problem for us for several years now. And I gather that you have some made progress with the -- specifically with the fusion centers in grant guidance, some. But unless I misremember, we still haven't gotten that far on grant guidance in general. And you indicated earlier that there were general process problems and legal issues related to this for the -- for the whole government.

Can we either now, or if it's easier maybe in a document somehow before next time, get more of an explanation of why it's so hard to, in essence, get this guidance at least for DHS entities -- not only sub-entities like the fusion centers or one that has another one, another one, another one -- because we have found, as you recall -- earlier reports, I think found that the Department would be

even more effective if some of these problems were addressed early on.

And grant guidance is exactly the way to do it before getting the grants, rather than trying to fix things later on. I'll get off my soap box now and let you respond.

Ms. Callahan: Well, to be clear, Lance, if it's a DHS entity, then they're under my purview. So that -- and that's my whole goal and philosophy as the Privacy Officer is to make sure privacy protections are instituted and implemented at the very beginning and throughout the process.

So the grants would only be provided to non-DHS entities. And that's attention that we have. I am not a grant lawyer. I am not a lawyer, actually, in this job right now. But I am specifically not a federal grants lawyer.

But I believe the problem is -- and we'll try to get you more clarity on this issue. The problem is to put on additional requirements that Congress has not expressly authorized. So it's a congressional mandate for us.

It's actually FEMA that provides our grants for DHS, so that the grants be provided by DHS through FEMA. And Congress puts on certain requirements within it.

And for DHS then to administratively add onto those requirements is, as I understand, difficult. The reason why we were able to do it with the privacy policy was because it was a timing element only, that it was -- it was associated with meeting a requirement that was previously required from the information sharing environment and from the fusion center legislation initially, which is why for CCTV, we had to go with the urge and encourage language or whatever the specific language is.

At the same time, we're trying to refine that to see how far we can push it. But that's my understanding -- is the tension is the branches in terms of who's authorized the money and for what purposes.

Ms. McNabb: And what we've been told on this long standing issue is it has to do with the

Paperwork Reduction Act in making changes to the grant application paper, I guess. And that it would -- there is a procedure that requires federal register notice and a whole big hullabaloo.

And you know, every year, we're out of the cycle for doing this. And so, what -- in my ravings on this topic earlier, what I was asking is for you to explore the possibility of using this urge and encourage approach if there's any way to get a general urging and encouragement to state level grant applicants to reveal whether or not their proposal would collect PII, and then collect that -- those -- that fact.

Now we know that X out of Y number of grants awarded last year did request -- did collect PII. And then we can look at that and see if you want to recommend something else, but just to find that out.

And our official filed report said that and then said more. So maybe just back off to just that, an unofficial urge and encourage.

Ms. Callahan: We'll see what we can do within

the scope of the law. And I think it's not just the Paperwork Reduction Act. I think it's lots of different elements. But that is one of the many hurdles we have in the Federal Government that I hadn't anticipated.

[laughter]

Mr. Purcell: Ramon?

Mr. Barquin: Mary Ellen, my question has to do with -- with best practices. I know we've speaking about it. And I know the subcommittees and the -- what do we do once we identify a best practice? And it's so important when you identify a best practice in any component in any specific, you know, report where someone is doing it right. What do we do with it to try to capture that as a process, disseminate it and ideally, in some way, capture in some type of a standard, you know, that everyone across the board, you know, if applicable, go do it?

Ms. Callahan: Well, and as you all know as privacy and security professionals, that creating a dialogue in a community and a conversation really

helps tease out what are the best practices. And together with the Component Privacy Officers, we've actually really started to engage on a lot of different issues and try to say, you know, we -- I think previously, Component Privacy Officers in the Privacy Office maybe even and other federal agencies kind of reinvented the wheel each time of, oh, we got a crisis. What are going to try to do?

And now what we're trying to do is anticipate what some of the issues are, and to try to have a conversation in a thoughtful way of how are you dealing with this issue. How are you dealing with this issue?

In terms of capturing it within the Department -- I mean, Toby talked at length about some of the best practices that -- in her words, that she's been doing within the Department. We're having a similar conversation in terms of dealing with specific issues and specific -- you know, whether it's Privacy Act disclosures or compliance or something like that.

And actually, we've been tasking component

officers to take the lead on different issues to try to memorialize that, so it's something that can go across the different components, whether it's in a policy format or in a best practices format, or whatever. And our new director of communications that I talked about in December and that Toby mentioned in passing, is also helping, for example, on the training side.

We have a lot of different training that goes on. And we're trying to leverage that to get the best of breed of each of the training so that we can have the best product and really, you know, use the Department's resources the way that they were conceived to be done, to be. You know, the sum is greater than the individual parts.

Mr. Purcell: And, Annie?

Ms. Anton: So first of all, I want to thank you for an excellent report that you gave us this morning. And you've had an amazingly productive year. It's just remarkable for your Department. So thank you for your efforts.

I also wanted to ask you a question

regarding the privacy policy reviews that you're doing for the fusion center policies. I was wondering -- it's a very kind of prescriptive activity. I'm wondering if the auditing is taking place after the fact to make sure that the privacy policies are actually being enforced.

Ms. Callahan: That kind of goes to the -- I think it was maybe Joe's point. And so, we're not at the point where we can audit, because we don't necessarily have the policies in place. A handful of the fusion centers do, you know, have the policies and have them in the final form. I do think that that should part of the conversation.

One of the questions I have, which we're still figuring out, is whether or not it's my office that does it or if it's some other venue that does it. But it certainly has been part of the conversation.

Another thing that we're encouraging them to do expressly -- you know, I signed the letter that says, yeah, you're at least as comprehensive as the baseline capabilities documents. And also

saying, you know, for your own analysis and review, you should think about doing a PIA.

Now a PIA is not required for the fusion centers, but in our -- we have two PIA's that are required. The first one was done about -- was December of 2008. And another one is required maybe at the end of this year. And in that PIA, we had encouraged people to do it.

There has been laudatory language about that. And I think that is a useful intellectual exercise for them to go through themselves, kind of in -- before there's a review or a process.

And in fact, several -- several fusion centers who are, you know, among the 10, have started to look into doing a PIA, which I think will help provide some rigor to this conversation.

Ms. Anton: I'd just like to -- just also note that when I think about enforcement, I don't think just about best practices or business practices. I'm really thinking about technical run time policy enforcement in the software. So I just wanted to note that as something more thinking about when you

do reach that point.

Mr. Purcell: And Dan?

Mr. Caprio: Thank you, Richard.

Thanks, Mary Ellen. I really wanted to commend you for your -- your leadership and your role, particularly within the CIO Council and the Privacy Subcommittee. I mean, that's all very encouraging. And there's, obviously, a lot of good things going on there.

My question is a little different, though. I mean, there's a lot of discussion of policies of, you know, e-health records, broadband, smart grid, notice of choice, of harmonization of -- of policy, both domestically and internationally, you know, the legislative component.

So I'm wondering, how -- you know, I'm sure you are, but sort of how you're involved with the process that's going on sort of within the White House and OSTP, sort of all the stakeholders and you know, your -- because your voice is obviously very important in that discussion.

And I know that, you know, lots of

different departments and agencies have a role. So I'm just wondering if you could speak to your role a little bit?

Ms. Callahan: Sure, sure. And actually, this gives me an opportunity to kind of follow-up on something that Toby said, which is kind of about the CIO Council and its structure.

And you know, there has been some question, and I believe there was even a recommendation last year by ISPAB to have a privacy council to be mirror to the privacy -- to be mirror to the CIO Council, kind of a raise it one level up.

I actually think right now, the privacy profession and where we are on technological issues -- it's better for us to be a committee as part of the CIO Council, because the CIO Council, as Toby mentioned, is dealing with a whole host of issues, many of them that -- technology based.

But kind of going back to Annie's point, you have to have the technology and the privacy protections integrated. And that's what Toby's Committee's doing, what the Web 2.0 Committee is

doing in integrating the privacy protections within the development of technological standards, like for example, crowd computing and so on.

So -- so in terms of the Privacy Committee and its role in the CIO Council, we have covered a lot of those topics and so on. With regard to some of the other issues that are taking place, there -- the -- there are a couple of interagency policy committees, IPC's, that deal with a variety of different issues.

For example, there's an Information Sharing and Access Interagency Policy, IPC, and the Privacy Guidelines Committee, which I am a co-chair, together with the ODNI Privacy and Civil Liberties Officer and the DOJ Privacy and Civil Liberties Officer. We are now a sub IPC of that IPC. And I know. Sorry about the acronyms.

But the interagency policy committee -- so we're engaged into that where there's lot of different issues. Similarly, we -- there is a cybersecurity sub-IPC on privacy and civil liberties. And so, those are integrated. The IPC

is themselves a really kind of the interagency decision making process on policy issues. And so, again, the two best examples are the cyber ones and the -- and information sharing and access ones.

With regard to the Department discrete issues -- and I'm not saying that it's not discrete. But with regard to like, for example, smart grids and with HHS and high-tech and their requirements, our office is not as involved into those implementations. But we certainly actually have had some cross-pollination and consultation on certain discrete issues, one being kind of anonymization and how do you deal with overlapping issues and overlapping data sets that may derive an individual identity, where the unique identity set isn't part of it. And that's also a conversation we've had in open government as well of the data sets being released.

So to answer your question kind of more generally is -- we're involved, particularly when there's kind of broader policy issues when there are discrete issues related to certain departments,

they're kind of dealing with it on themselves. But given the other activity, I think we're informing -- I think the entire federal privacy community is informing each other both on technological developments and on other privacy impacts.

Mr. Caprio: Thank you.

Mr. Purcell: Mary Ellen, thank you. I think the -- speaking for myself, and I hope the whole Committee, there is a certain level of delight to understand better the conversation and dialogue across the federal space that involves, not just privacy, but security, information sharing, that the component parts of the framework of the federal government information management systems -- that you're at the table with your staff through these processes is vitally important.

And one of the things that I would agree strongly with is being part of the CIO Council is very important. And actually elevating that could put you into a dialogue with only yourselves.

Ms. Callahan: Right.

Mr. Purcell: And not with all these other

stakeholders. And we have to keep remembering that privacy is a component part of a large trust model that involves technology and broader policy decisions, as well as procedural decisions.

So we have -- we encourage that continuing effort to be at the table for these broader discussions as well. Thank you, very, very much.

Ms. Callahan: Thank you, thank you. And if I can add one final plug, which is that no one can replace Toby, but we're going to have to try. And her position is currently being advertised in usajobs.gov.

So please encourage, you know, as many qualified people to apply as can be. I really want this to be -- as I said to Toby, I think she has the best privacy job in the government, because she gets to deal with all these crazy, awesome, really interesting issues, and doesn't have to do administrative work.

And so, we really do want to make this a signature position, if you know anyone who's interested.

Mr. Purcell: Thank you very, very much. I wanted to specifically thank you again, Mary Ellen, for speaking with us today and being as open and accessible as you've been.

To Admiral Brown for his comments today, to Toby for giving us a better view into the broader space of the Federal Government.

To those who have joined us today, thank you very, very much. This concludes the public portion of today's meeting.

Committee members, thank you for your attendance and engagement today. And we look forward to quite a bit more.

The transcript and the meetings of this -- of the minutes of this meeting will be posted as soon as they're available. Please check that Web page frequently. If you haven't subscribed to the -- to the feed from our own Web site, please do so. And as of that, I conclude this meeting.

Please -- please -- pardon?

Male Speaker 3: --

Mr. Purcell: The public portion of the

meeting. We need to retain the Committee's attention for some minutes following this public portion. Thank you all very much. Meeting adjourned.