MEETING OF THE

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

Tuesday, May 25, 2010

United States Government Printing Office

Harding Hall

710 North Capitol Street, NW

Washington, D.C. 20401

The meeting was convened at 12:34 p.m., RICHARD PURCELL, Chair, presiding.

DPIAC COMMITTEE MEMBERS PRESENT:

RICHARD V. PURCELL, Chair, presiding
ANA I. ANTÓN
J. HOWARD BEALES, III
DANIEL W. CAPRIO, JR.
JAMES W. HARPER
KIRK HERATH
DAVID A. HOFFMAN
LANCE HOFFMAN
JOANNE MCNABB
CHARLES PALMER
NEVILLE PATTINSON
JOHN SABO

Also attending:

MARY ELLEN CALLAHAN, CHIEF PRIVACY OFFICER AND SPONSOR

MARTHA K. LANDESBERG, EXECUTIVE DIRECTOR AND DESIGNATED FEDERAL OFFICIAL

PROCEEDINGS

MS. LANDESBERG: Good afternoon everyone and welcome to the second quarterly 2010 meeting of the DHS Data Privacy and Integrity Advisory Committee. I welcome you. I'm Martha Landesberg, Executive Director of the Committee. And with that, I'll turn the meeting over to our Chairman, Richard Purcell.

MR. PURCELL: Thank you Martha. And welcome all to the committee meeting. We have, I think, a very full and exciting agenda for the afternoon. We'll handle it as quickly as we can.

The housekeeping rules apply, as always. Which include, first and foremost that mobile devices should be put on as silent as possible mode. Those who don't do that, we have a room in the back for you, all prepared.

At the end of our time, we reserved time for public comments. Any of you who are interested in addressing the committee at that time, please sign up at the table outside this room. We always welcome and encourage those comments so please feel free to sign up. But you must sign up prior to making your comments to the committee.

At this time, I'd like to welcome our Chief Privacy Officer of the Department of Homeland Security, Mary Ellen Callahan. Prior to joining DHS Ms. Callahan was specializing in privacy, data security, and consumer protection law as a partner at Hogan & Hartson here in Washington, D.C..

Mary Ellen has served as the co-chair of the Online Privacy Alliance, which was an industry self-regulation group. Also as vice-chair of the American Bar Association's Anti-Trust Division Privacy and Information Security Committee.

With the Privacy Office at DHS, Ms. Callahan is responsible for privacy compliance across the entire department. She also serves as the Department's Chief Freedom of Information Act Officer.

Ms. Callahan, please proceed.

MS. CALLAHAN: Thank you very much Chairman Purcell. How's my mic, it's okay?

MR. PURCELL: Getting better.

MS. CALLAHAN: Excellent, excellent.

STATEMENT OF MARY ELLEN CALLAHAN, CHIEF PRIVACY OFFICER, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

MS. CALLAHAN: Thank you very much and thank you Committee members for being here today. Thank you to the members in the audience including several of the privacy officers throughout the Department of Homeland Security's components. As well as privacy officials from the Department of State. So we've got a great representation of the interagency process that we hope to foster on privacy issues here at DHS.

We are going to have a slight change in the agenda. I will give my remarks and give an update on the activities since we last met on March 18th. And then upon the arrival of the Secretary, I will stop my remarks and then conclude them upon her departure.

She is, as I mentioned to several of the Committee Members, at the retirement ceremony for Commandant Thad Allen, who is retiring as the Commandant of the Coast Guard, but will remain as an Admiral in the Coast Guard for the duration of his activities, I believe with regard to the Deepwater Horizon issue.

So she will be -- she is on her way from there. But in the meantime, I have a lot of very exciting things to talk about, what the Privacy Office has been doing in the past two months.

First, let me explain that we are going to be hearing from the Secretary about privacy and security issues and her vision for the Department of Homeland Security. Last meeting, I mentioned that we have a new Senior Analyst.

Helen Foster has joined us and has really hit the ground running, specifically addressing information sharing issues. And she will provide a briefing on developments in information sharing governance in the Department, including revised DHS guidance documents and the Department's response to the Committee's White Paper on Information Sharing and Access Agreements.

Next we'll hear from Lyn Rahilly, the Privacy Officer for the U.S. Immigration and Customs Enforcement. This is part of a series of presentations to the Committee that I hope to commence to have you understand how the privacy officers in the components are working day in and day out to make sure that privacy is addressed early in the development of a program to make sure it's systematizing privacy.

As you know, last June the Deputy Secretary instructed all the components to have privacy officers has well as NPPD, I&A, and S&T. Seven operating components do now have privacy officers, and the other three are well on their way to finalizing that.

Lyn is a great example of how much a privacy officer makes a difference in the implementation of privacy principles and fair information practice principles into the system. She came on board in early 2008, and really has revolutionized the privacy approach in ICE. And so I look forward to hearing her presentation today.

And then in the final session we're going to be joined by Ely Kahn, who is a Director of Cybersecurity Policy on the White House National Security Staff. Ely will be providing an update on the National Strategy for Secure Online Transactions.

And I'd like to thank Ely and our presenters for making time in their schedules to discuss these important issues and specifically, the important interagency effort on secure online transactions.

With regard to the Office, as always, we have a lot of exciting developments in the Privacy Office to report. We continue to strive to raise awareness about the Privacy Office and how privacy issues are relevant to all aspects of the Department’s work.

We'll soon publish our Privacy Office Guide, which will describe how this office carries out its duties and responsibilities, and, perhaps, be a primer for other Privacy Offices as they attempt to stand up a comprehensive privacy program within the Federal Government.

We have also re-launched our internal intranet page on SharePoint and have established a comprehensive privacy and FOIA training resource page for our employees. We've also revamped our external website to make it easier for the public to access our privacy and FOIA resources.

Hopefully, you've taken a look in the past couple of weeks. As you know, this was one of my first initiatives when I started, and I am thrilled with the increased transparency and increased ease of use of the website. So I encourage you all to take a look at that.

And we will continue to work on updating our compliance-related web pages to provide better transparency into the compliance process and to make it easier to locate important privacy documents including PIAs and SORNs.

Steve Richards, our Associate Director for Training and Communications has taken the lead on these efforts. And I thank him for that, for helping to work on increasing the comprehension, and visibility, and transparency of the materials that are available on the DHS privacy website.

Next month, consistent with the transparency theme, we are going to begin a series of monthly Chief Privacy Officer articles on the DHS Blog, to further expand our outreach to the privacy advocacy community and the general public.

With regard to compliance, as you know, I always call it our bread and butter, and it is indeed that. They have been hard at work on reviewing Department systems and programs through the Privacy Threshold Analysis process, and overseeing the drafting of PIAs and SORNs. Since the Committee has last met, we have approved 130 PTAs, 14 PIAs, and 5 SORNs.

We’ve also hired a new compliance analyst, for the compliance team, who should join us shortly, and an administrative assistant, Erin Odom, has been assigned to the group to help with the workflow of documents. So I think that that will really help institutionalize several of our compliance elements.

In addition, Compliance is gearing up for our annual Privacy Compliance Workshop, entitled Pieces of Privacy, which will be held on June 10th here in Washington. The workshop will provide training on triggers that indicate the need for privacy compliance documentation, Privacy Act requirements, and computer matching agreements. And we're also introducing a format to include speakers from other DHS offices and government agencies to provide additional guidance.

We’ll also debut our PIA template and corresponding guidance that I have discussed with the Committee in the past. I'm very excited about this. This again was another initiative that I had focused on upon my joining DHS in March of last year.

The new template will hopefully provide greater clarity and demonstrate the level of analysis and rigor that has taken place in the Privacy Impact Assessment process. And to make sure that we provide even further transparency with the PIA documents.

We have also been coordinating with USCIS Privacy and the USCIS Transformation Office, which is building an immigration system that is person centric rather than form centric. We are working with the program to build privacy in at the very beginning of the system’s development.

And I think this is a good example of ways to collaborate and to leverage different privacy resources to make sure that privacy considerations are indeed taking place.

The way that we're working on this is that

Shannon Kelso, one of the compliance analysts, is going and spending a week -- a week at Transformation often in collaboration with USCIS Privacy to talk about what privacy issues have been addressed during that week and what are the issues.

Shannon will then join Director of Compliance, Becky Richards, to address these issues every two or three weeks so that we can resolve the privacy issues on a periodic or a seriatim basis as the technology is developing. Because Transformation is a very heavily technological process, we want to make sure that the tools are built in to make sure that privacy is protected throughout these processes.

We've also been working with the Screening Coordination Office, who you heard from two meetings ago, the CIO's office, the CIO for I&A, for Intelligence & Analysis, and the Office of the General Counsel on a business case for developing a technical and policy framework for using data in both the classified and unclassified setting, and for sharing information within DHS and with our partners.

The goal of this effort is to provide

protection and control of DHS data through policies and technical methods to better achieve operational needs while at the same time meeting legal, privacy, and technical requirements. I'm very excited about this and I hope that this will be a successful, a successful product in the near future.

We're also actively -- we're an active member of the DHS New Media Compliance Working Group, which provides guidance on implementing social media. The group will review every proposed social media tool or initiative in the Department.

Other members include Office of the General Counsel, Civil Rights and Civil Liberties, Office of Public Affairs, the Chief Information Security Officer, and of course, the Office of Records Management.

Our specific goal is to establish a compliance process for ensuring that privacy is built into the Department’s social media initiatives before they launch.

And going forward, I am working with the compliance team on another of my initiatives for this year, which is to systematize how we review our ongoing programs for compliance. And by that I mean compliance with DHS policies, procedures, and public statements, including PIAs and SORNs. We'll have more on that issue in September.

With regard to privacy technology and intelligence, my office is working very closely with the Office of the Chief Information Officer to publish DHS data sets to the Data.gov website. We assist in the internal review process for all proposed postings of data sets, to ensure that DHS does not publish PII.

I am also pleased to report that we are, of course, giving serious attention to the recommendations in the Committee’s report on improving the PIA process for Service Oriented Architecture.

We plan to use the report to create a new privacy threshold analysis document to conduct initial assessments of the privacy impacts of Department Enterprise Service Buses, and to create a template PIA to standardize privacy protections for ESBs used across the Department. We thank you for the guidance in this area, of course.

We also, with regard to opportunities at the Department that the office has been engaged in, as you know, for the past year we've been reviewing products from the Office of Intelligence and Analysis that are distributed to fusion centers and to other State and local colleagues.

In light of the ongoing threats, I wanted to report that the number of products that we have reviewed since March 18th, since our last meeting, has increased. And we've reviewed 73 products and 200 Homeland Intelligence Reports.

We continue to improve our privacy incident management processes and try to systematize them throughout the Department as well. On March 24th, the Deputy Chief Privacy Officer Kropf and Director of Privacy Incidents and Inquiries, Rose Bird, who testified here two meetings ago, met with privacy officials at the Internal Revenue Service for a demonstration of their Privacy Incident Management Online Tracking System, and to share best practices.

Rose will also present an overview of recent privacy incidents during the third DHS Privacy

Incident Handling Quarterly Meeting in June. This is required by OMB and of course, the forum provides an opportunity for component privacy officers, privacy points of contacts and DHS Enterprise Operations Center managers to share information and provide feedback with regard to privacy incidents, privacy management, and mitigation and prevention.

We are also currently investigating a component data breach that has significant policy and legal violations. My incidents team may release a public report on best practices at the end of the investigation.

With privacy training, as you know, that again is something that I want to encourage to make sure that privacy is systematized and considered throughout the Department. We've engaged, led by Steve Richards again, in an intensive effort to enhance the Department’s privacy curriculum.

We're upgrading our online Culture of Privacy Awareness course, we're upgrading right now, which all DHS employees are required to take annually. We've also recently rolled out new versions of other

Department-wide privacy courses:

The introduction of DHS privacy policy and FOIA that all new employees receive as part of their initial DHS orientation; and the privacy compliance program of DHS 101, the Department’s comprehensive course on DHS operations that's open to all employees.

We continue to be deeply engaged with the national network of fusion centers. Since our last meeting, my office, in close coordination with the Department’s Office for Civil Rights and Civil Liberties, rolled out its first two installments, actually first three installments since the third is going on right now, of our Train the Trainer Privacy and Civil Liberties training at regional fusion center conferences.

Those conferences have taken place in Portland, Oregon, Montgomery, Alabama, and a third session is taking place right now in Minneapolis, Minnesota. The fourth is scheduled for Philadelphia next month.

As we discussed previously, each two day

Train the Trainer course focuses on: helping fusion center privacy officers understand the full reach of their responsibilities; giving them an overview of federal privacy laws, policies, and concepts like the Fair Information Practice Principles and how they can be implemented in their centers; and introducing them to training materials that they can use back in their centers when developing and delivering their own privacy and civil liberties training.

This is, of course, just the beginning of the conversation on privacy and privacy officers in the fusion center. As a condition of receiving their training, these privacy officials have committed to delivering privacy and civil liberties training at their home fusion centers within six months.

In turn, we've promised to continue our technical assistance and do everything we can to make their training a success including possibly going to observe, to provide information, to provide further assistance.

We have great hopes for this training, and believe it is another important step in sharing our culture of privacy with the fusion centers and helping to take ownership of privacy at the local level.

We will also continue to support privacy training by visiting fusion centers in 12 states by the end of the year to provide more detailed, comprehensive training for the fusion centers. That is in addition to, not to replace the training that each of the fusion center privacy officials are required to provide.

Furthermore, as you know, and as I've discussed previously, the Information Sharing Environment requires all fusion centers to have privacy policies that are, "at least as comprehensive" as the Information Sharing Privacy Guidelines. And my office is reviewing those -- the fusion center privacy policies on behalf of the ISE Privacy Guidelines Committee.

To date, we've issued 15 approval letters to fusion centers stating that they've met the standard laid out in the guidelines. We expect a steady increase in the number of policies we are sent to review. We will support the fusion centers in any way we can and continue to encourage them to take advantage of technical support that's provided.

As you may recall, the Department of Homeland Security has required, in their FY 2010 Grant Guidance, that the fusion centers, if they are receiving grant funds, must complete a privacy policy that is reviewed by and approved by my office within six months of receiving FY 2010 funding. They should be receiving that funding within the month.

So the clock has started to tick. And we have several that are in the pipeline, they are just not yet in my office for review. So I think that having this deadline has been particularly effective and appropriate to focus on the privacy and civil liberties issues in the fusion center.

While the privacy policy is just the first step in this dialogue, it's an important step and one to lay out the parameters associated with privacy and civil liberties protections in the fusion center and to be the basis for the privacy training.

We continue to be extraordinarily busy on the international front. Here are some of the highlights. And I think the Secretary is probably in the elevator, so I may cut this a little short.

April 19th to the 22nd, we hosted representatives from Justice Canada, Spanish Ministries of Interior and Justice, and the German Ministry of Interior. We were hoping to have somebody from the German DPA, the Belgian Ministry of Interior, and the Hungarian DPA.

But unfortunately the volcano -- that was the week of both IAPP and of the volcano and so they were unable to travel from Europe. But fortunately, our Spanish colleagues were able to get out that week. Along with, of course the Canadians, and the German was already here.

The presentation that we had with the international fellows was part of our ongoing Privacy Exchange Program, to demonstrate the U.S. privacy framework and how it governs DHS' privacy policy along with the Federal, Executive Branch privacy structure.

I am very pleased to report that the State Department's International Visitor Program is starting a program similar to ours, and we're assisting in the development of this curriculum. But that's a great way and an appropriate way for State to have this dialogue on privacy issues and how it is a foreign policy issue in terms of privacy policies.

Our international team, together with the Departments of State and Commerce and the Federal Trade Commission, has contributed to the efforts with the OECD Volunteer Working Group to plan upcoming events celebrating the 30th anniversary of the OECD Privacy Guidelines, including of course, a privacy conference in Israel in October.

We are also conducting research on public sector implementation of the OECD Privacy Guidelines, and hope to complete it in time for the 30th Anniversary celebration. Our project complements work the Department of Commerce is doing on private sector enforcement.

We hope both projects will inform the OECD Secretariat’s decision on how to move forward with its review of the Guidelines. And I think that that's an important bookend to the work that the Department of Commerce is working on as well.

In addition, countries that wish to join the Visa Waiver Program, as you know, must sign a Preventing and Combating Serious Crimes Agreement, or PCSC, with the Department of State and the Justice Department. On May 6th, I met with the Belgian PCSC delegation to discuss U.S. and DHS Privacy considerations.

My international team has worked with US-VISIT and with the Government of Germany to discuss the flows of data relating to CJIS that is shared under the PCSC Agreement.

MR. PURCELL: Mary Ellen, one moment if you would please.

MS. CALLAHAN: I believe the Secretary is here.

MR. PURCELL: Members of the Committee, will you join me in welcoming the Honorable Janet Napolitano.

[Applause.]

[Whereupon, the Secretary greeted the Committee Members.]

MR. PURCELL: Madame Secretary, welcome to this meeting of the Data Privacy and Integrity Advisory Committee. Mary Ellen, if you wouldn't mind making further introductions please?

MS. CALLAHAN: Absolutely, I'd be happy to. Thank you very much Chairman Purcell, and Madame Secretary, welcome. I would provide a brief overview of your fabulous career if I could. I know you're making a face, but we'll go quickly.

As the Secretary of the Department of Homeland Security, Janet Napolitano is leading our nation in the collective effort to secure our country and the range of threats we face, from terrorism to natural disasters. She's charted an ambitious new course for her Department and its more than 225,000 employees.

She has forged international agreements to provide more tools in the fight against terrorism; instituted new, more effective strategies in immigration enforcement; accelerated recovery efforts in the Gulf Coast region; and initiated sweeping reforms to transform the Department into a smarter, leaner, more efficient agency.

Prior to joining President Obama’s Cabinet, Secretary Napolitano was serving in her second term as the Governor of Arizona and the first woman to chair the National Governors Association. Previously, she has served as Arizona Attorney General and as U.S. Attorney for Arizona.

Madame Secretary, I was just discussing our international privacy initiatives, which I know is near and dear to your heart. But I would like to -- please everyone join me in welcoming -- in welcoming the Secretary of Homeland Security, Janet Napolitano.

SECRETARY NAPOLITANO: Thank you.

[Applause.]

STATEMENT OF THE HONORABLE JANET NAPOLITANO, SECRETARY OF HOMELAND SECURITY

SECRETARY NAPOLITANO: Well thank you Mary Ellen for leading our Department's privacy efforts. I want to thank everyone for being here. I know this Committee is normally able to meet without this sort of commotion, so I appreciate your willingness to have me here this afternoon.

What I'd like to do today is discuss a few points about privacy, the Office of Privacy, and the role of this Committee. And then open it up, if I might, Mr. Chairman for questions.

And first of all, the specific role of the Privacy Office and this Advisory Committee is essential in the Department of Homeland Security. It's particularly essential in several respects that I'm going to detail here in a moment.

But as Mary Ellen knows from meeting with me, from traveling with me, this effort and the efforts to make sure that we consider privacy and civil liberties at all aspects of our operational initiatives from the beginning to the end is something that is fundamental to my role as Secretary.

And I think it's fundamental to make sure that we're asking questions, we're probing some of the initiatives that we're doing, and really taking careful thought of, quite frankly some of the balances that have to be struck given some of the security needs that we have both nationally and, particularly, internationally.

Most of you have been experts for a long time. I don't need to belabor some of these points. But I do think it important to bring to this Committee's re-attention, I know it's been at your attention, but your re-attention, is that everything we do to combat terrorism or violent extremism is rooted in the fundamental reason why we're in this struggle to begin with.

And that is to protect and secure American values and the American way of life. And that means for now and for future generations. And our values include our freedoms and our privacy. And so we always have to be thinking about how those things can be preserved, protected, and indeed embraced as we move forward.

I believe that we need to cast aside the dichotomy between liberty and security or between privacy and security. I think there are ways that we can achieve both. And I think that's very important that we announce at this Department that we are not going to live with that false dichotomy, we're moving forward, really thinking through how initiatives can be changed, how technology can be adjusted, how things can be carried out.

Now let me, if I might, as we move forward in what has become a very fast moving and ever evolving threat environment, it is not static, but it is ever present. And if anything, the threat environment has become more intense and acute even during my time as Secretary.

And that is all the more reason why it's important to have a strong Privacy Office within the Department of Homeland Security. It's there to make sure that we properly integrate these values at the beginning of initiatives. It's there to make sure that we develop new technologies and new ways to use existing technologies to make the nation safer, to make our citizenry safer, but in a way that honors the need for privacy.

The Privacy Office is not just a box on our organizational chart that's kind of out there, you know, as you check the box in an org chart. It is there as a fundamental part of the organization even as we send out new initiatives, whatever -- across the world and across the country.

I know that Mary Ellen's going to update you about the activities of office later on in the meeting. But it is a strong, front line presence in our efforts to protect the country. It provides invaluable advice to me, when I say “it,” it's the Chief Privacy Officer.

And they have, through the Privacy Threshold Analysis and Privacy Impact Assessment process, a way to make sure we are overseeing proposed and redesigned systems and protocols at the outset, rather than shoe horning them in at the end.

We want to make sure, and the Privacy Office makes possible our confidence that we are in compliance with the major pieces of legislation that Congress has expressed in order to protect our privacy values, namely, the Privacy Act and the E-Government Act.

It also has helped ensure our compliance with Executive Branch directives, including the OMB Privacy Guidance and the Fair Information Practice Principles. The Privacy Office is in charge of making sure that we are complying with the President's Open

Government Initiative.

And that we also take a transparent -- an expansive view of transparency. This includes all of the reporting required by the Congress. It includes making our Privacy Impact Assessments available to the public. It includes holding public workshops and preparing reports on cutting edge privacy issues.

It includes direct outreach to privacy advocates and other stakeholders. And it includes making sure that the American public has access to our Department's actions regarding privacy through a new and better website.

Not only does it hue to this broader spirit of privacy and also transparency, but it works with the components to proactively disclose information. Thanks to the Office's leadership, the Department has made significant enhancements to our online FOIA Reading Rooms, which helps provide transparency into the types of documents being requested by the public.

We also are providing essential privacy training to all DHS employees, and to employees of other Federal agencies. We are supporting our colleagues in State and local fusion centers with guidance and training as to how they develop their own privacy policies. So it's not just for Washington, D.C., it's for efforts across the country. And it oversees our response to privacy complaints.

In addition, the Privacy Office is serving as the senior advisor to me on international privacy frameworks and policies, which we increasingly seek to harmonize as we take a more international approach to combating the threat of terrorism.

In other words, we understand that many of the terrorist threats against the homeland begin overseas and we have to have ways to exchange information and do so in a fashion that complies with international privacy and data collection principles and protocols.

So the mandate of the Privacy Office is very broad. It needs the best counsel we can get to deal with these issues. And as an office that must look out for the interests of the American people, we need input from the public. This is to make sure, to be a check, to make sure we are ensuring the values that we are stating verbally and in writing. So that's the role provided by this Committee.

I'd like to thank you for your work and your guidance in the many critical aspects of our work. We are grateful to have the benefit of insights from this distinguished group of legal, privacy, and technology experts representing a broad range of perspectives, small and large business, non-profits, academia, and State government.

Since it's been established, this Committee has issued 11 reports providing guidance on implementing privacy policies and programs, and on best practices. And the work of this Committee has itself helped to guide and direct this very new department.

And when I say very new, in the Federal scheme of things, we're very new although we are now the third largest department of the Federal Government, and in some fundamental respects, the one that touches the American citizenry most often and most directly.

Your work on the Secure Flight and E-Verify programs has led to changes in how those programs use personal information and, in the case of E-Verify, it has changed the way that the identities of the program's users are authenticated.

This Committee has improved the Department's interactions with the members of the public who use the E-Verify program. And when we look at the work that has been done with the Committee and who is on the Committee, we do so with appreciation of what you have done and also appreciation for the important role we are asking this Committee to play.

I understand that you're going to be receiving an update on the Privacy Office's role in shaping the Department's governance structure for information sharing agreements with external partners.

And I want you to understand that in devising that role, the Privacy Office has actually used the 2009 White Paper about embedding privacy protections in the Department's Information Sharing Access Programs.

And as all of you know, or I hope know, the redress programs are also important and important to me. We want to make the redress programs more transparent, efficient, responsive and easy to use. And we are looking carefully at your report from earlier this year on that topic.

We also have no doubt that your report on privacy protections for our IT infrastructure will prove invaluable to our efforts in that area.

So let me conclude by thanking you for the contributions you have already made and the guidance that you have already provided. And for the window on our operations that you provide to the public. We all have an important and dual responsibility, securing our country, and protecting our values.

And as I said earlier, they are not in conflict with each other unless we insist that they be in conflict with each other. And our goal ought to be, to be able to pursue both of those things simultaneously.

Thank you for your service. Thank you for lending us your guidance and expertise. Thank you for what this Committee has done and what I'm sure you will be doing both now and in the future. I appreciate it. Thank you very much.

MR. PURCELL: Thank you Madame Secretary.

[Applause.]

MR. PURCELL: Thank you very much for those comments. I'm going to take the prerogative of he whose tent doesn't have to be upended to ask a question.

You mentioned earlier, and I applaud numerous mentions of embedding privacy as a design principle in services, products, technologies, and also the need for international cooperation.

I wanted to just ask a question of, how to resolve that with the negotiations that have gone on and continue to go on through the good offices of both Mary Ellen and Mr. Kropf on the international desk with the PNR and the SWIFT negotiations, difficult negotiations.

And what you've said today and what we believe about the trade-off between security and privacy comes into play particularly with our European friends, to a certain degree. They do make a certain allowance of measure, of balance between those as well.

So how will you be guiding the pursuit of those negotiations over the next six or more months as we try to resolve the current impasse that we're at?

SECRETARY NAPOLITANO: Well, let me divide it into two parts. On the SWIFT Agreement issue the Department of Justice is taking the lead on those negotiations along with the Department of Treasury. We are providing some input there.

The Attorney General and I were in Spain a few months ago meeting with members of the European Commission. And this topic, of course, was one of the topics that came up, and with Representatives of the European Parliament was well.

We're now in the post-Lisbon Treaty world and the European Parliament has to be an important aspect of these discussions and negotiations on many, many things. We have divided the world because SWIFT mostly impacts Justice and Treasury more so directly then DHS, they are taking the lead there.

PNR, we have found and it is, I must say in my year and a half as Secretary now, that when you look at airport and aviation security, you have to look at it in several ways and in multiple layers.

One set of layers that's very important is information about passengers before they even arrive at the airport, so that decisions about screening and secondary screening and so forth can be more intelligence based as opposed to, say for example, what we had to do after Christmas which was to adopt what is now known as the 14 Country Rule.

That intelligence based and passenger based focus requires, I think, that we have PNR/API agreements. And that not only do we have them, but that we move to achieve some consistency in them across the globe. Because the plain fact of the matter is that we don't just benefit from them, the citizenry of other countries benefit from them.

And it's not just about terrorist commission of trans-national crimes. You know, criminals, money launderers, drug traffickers, and others, human traffickers, using the airlines and the aviation system to move about the globe. So everybody has an important stake in this. So that's one aspect of it.

The second aspect of it is that the more robust kind of information sharing on passengers, the more confident or the more applicable all the different changes in airport technologies themselves are. And so that the layers all work with each other, better information, intel driven about passengers and newer and better screening technologies moving forward.

You are right that our European friends have raised a lot of questions about PNR. And one of the key things there, Mr. Chairman, is to educate them on all the privacy laws and protections that exist in the United States.

And so Mary Ellen, as the Chief Privacy Officer, has done a lot of one-on-one briefing going back and forth. We have invited several of the new leadership over here so they could see, for example, the National Targeting Center and how that work is actually done and how the data actually is protected.

I hope with the understanding of mutual need and greater understanding of the importance that we place on privacy, that we can begin reaching some consistency, particularly with the EU.

MR. PURCELL: Thank you very much.

Mr. Harper.

MR. HARPER: I wanted to join in thanking you for coming to visit with us today. It's important to us to have you here and important to the DHS community to have you here because it signals that privacy is important, the work that Mary Ellen does is important.

No good deed goes unpunished, so as a token of thanks --

SECRETARY NAPOLITANO: Oh boy, a book.

MR. HARPER: I wanted to offer a book that I was a co-editor of that actually came out yesterday, coincidentally, from the Cato Institute. It's called Terrorizing Ourselves, Why U.S. Counter-Terrorism Policy Is Failing and How to Fix it.

It's a little bit of a provocative subtitle, but it's a book about terrorism where we tried to capture it strategically, tried to understand terrorists and their motivations, talk about risk management and cost benefit, which is so important to address the twin threats of terrorism:

One being the attacks themselves, and the other being overreaction in response. Where we might waste our own blood and treasure, push people toward the side of terrorists by our overreactions, and so on and so forth.

And then the final two chapters are on communications, which I think could be very valuable to a person in your position. To ways of thinking about talking about these problems so that we don't overreact. So that we do put ourselves in the position to carefully balance all our interests, including security, and privacy, convenience, financial well being and so on and so forth.

SECRETARY NAPOLITANO: Very good.

MR. HARPER: So thanks very much for being here. If it's not an abuse of the privilege --

SECRETARY NAPOLITANO: Did you autograph my copy? I want you to autograph my copy.

MS. CALLAHAN: Did you sign it, Jim?

MR. HARPER: I did sign it. I did sign one that I'll give to you. I'd like to segue into a question where I think we may have a good example of a program that is overreaction. That is, spending that doesn't have a security, a strong security gain and that has threats to privacy and civil liberties.

And that came to my attention again in last week's GAO report on the SPOT Program. The Screening of Passengers by Observation Techniques, where behavior detection officers in airports try to pick out people.

If the GAO weren't so kind and subtly state it, I think this report would be rather damning. Because it points out that there's no scientific basis for this program, that it was adopted, not during your tenure, but it was adopted without risk assessment or cost benefit analysis.

And that of a 152,000 secondary referrals, only 1,100 have resulted in arrests, less then half of which might have anything to do with terrorism, and zero actual terrorists have been caught while 16 terrorists have passed through SPOT protected airports.

It's a big report, I don't know if you've had a chance to review it and look through it. But I wonder if you have any comments on the GAO report or on the SPOT Program and BDOs?

SECRETARY NAPOLITANO: No, I haven't had chance to review that GAO report. We get a lot of -- GAO's a pretty -- they look at a lot of things in our Department and we try to have people review them and derive from them changes or things that we should be doing in reaction. So while I don't know the name of the particular people that are reviewing it, I know it is being reviewed and ultimately that will get up to me.

I do think, however, that it's important for the Committee to recognize that the SPOT Program is based on a similar program employed in Israel and other countries. We are not alone in using something of this sort. And we don't rely on it as the sole means of protecting the aviation environment.

That's why I said before, the more we can deal with advance passenger name information and in a way that allows things to be checked almost before a passenger gets to the airport for a flight, the better off we are. That's why these API/PNR Agreements are so important.

But when they get to the airport and the actual physical environment of the airport it's multiple layers and it's about terrorists, but it also about a whole lot of other things that can be a danger in the aviation environment. From potentially violently disruptive passengers, to those who are carrying drugs or other material, et cetera, et cetera.

So we will carefully review the GAO report. We will carefully assess whether, you know what, maybe there are changes in this program that should be made. And we will look at what metrics they use to measure the program versus some other metrics that the Department may be using to measure the program. And then we'll make adjustments as necessary. Nothing that we do is engraved in stone.

MR. PURCELL: Thank you Madame Secretary. Are there other questions, comments, or shameless self promotion?

MS. CALLAHAN: I think we have time --

MR. PURCELL: Mr. Sabo.

[LAUGHTER.]

MS. CALLAHAN: Richard, I think we have time for one more question or shameless promotion.

MR. PURCELL: Last one.

MR. SABO: I would ask you to co-author my next book.

[LAUGHTER.]

MR. SABO: Just a comment and a kind of a suggestion. And you referenced the E-Verify report and others. So much of the policy work, the great work that Mary Ellen and team have been doing, from policy perspective and from perspective of compliance, in the end has to rely -- and training, in the end has to rely on systems to implement the controls that ensure privacy and ensure security. And we run into that all the time, and the E-Verify is one example, and others.

And my suggestion is, that within the span of the Department, you've got S&T, you've got an R&D budget for example, and grants. There's a lot of great work going on in the university environment, in the private sector standards organizations to look at technical mechanisms to improve privacy management and compliance.

And my request is that, as you look at your S&T budget and research, look for or perhaps request proposals for research grants, or for pilots, or for studies to perhaps implement work underway in the university community on privacy management that looks forward a little.

Isn't just looking at policy but is actually looking at ways to more effectively deliver privacy. So just a suggestion. I know a lot of the research budget is on particular tools to you know, help solve particular problems. But there's ample room for that type of research.

SECRETARY NAPOLITANO: I think that that is a very thoughtful and interesting suggestion. Because at some point, we push the envelope about what the American public is willing to tolerate, right, by way of inconvenience and the like.

And the American people are pretty tolerant if they think something is really directly linked to protection and safety. If they don't think it's linked to protection or safety, you get to the point you were making which is, overreaction and is something really connected to risk evaluation and the like. So that's one issue.

And the other is that, as I said in my comments, what this fight is about is protecting American values. And we need to be kind of leaping forward a little bit in terms of not just what we're doing now, but really getting some minds just focused on -- for example, what is the next -- what does the 21st Century, or 22nd Century airport environment -- what should that look like?

Or how do we make sure, with privacy protections built in, that employers are hiring those who are legally in the country. And you know, there are all kinds of other questions that we have. So I think that is a very interesting and good suggestion and I'll talk with Mary Ellen about it when we get back.

MR. PURCELL: Madame Secretary, thank you very much for joining us today. It's a delight and a pleasure to have you. And it is very important to the Committee and to the broader privacy community to know that the commitment you have to privacy is genuine and sincere. Thank you very much for your time today.

SECRETARY NAPOLITANO: It is, and I appreciate the opportunity to be with you. Thank you all very much.

MR. PURCELL: You're welcome and thank you.

[Applause.]

MR. PURCELL: Mary Ellen, thank you for your indulgence during the interruption of your boss. You may proceed, please.

STATEMENT OF MARY ELLEN CALLAHAN, CHIEF PRIVACY OFFICER, UNITED STATES DEPARTMENT OF HOMELAND SECURITY (CONTINUED)

MS. CALLAHAN: Thank you very much Mr. Chairman, and thank you Committee Members. She is, indeed, my boss and so I am happy to step aside for her for just a brief half hour.

She was talking about -- I paused when we were talking about international issues and I wanted to just pick up that thread before me move to just a few more items in my presentation. And then I am available for questions as well and perhaps some gratuitous promotion as well.

MR. HARPER: I have a copy of the book for you Mary Ellen.

MS. CALLAHAN: Did you autograph it? Is it autographed to me?

MR. HARPER: [Nodding.]

MS. CALLAHAN: Okay, good. The one final point on international issues is that my office has issued a memorandum to all the components to integrate international privacy training in their training for outbound attachés and liaisons because as I mentioned, privacy is often used as an international or foreign policy dialogue or tool.

And the training is to raise awareness among DHS personnel on the legal and policy issues, and also to have a comprehensive approach to privacy among the component and department attachés and liaisons.

The Secretary spoke on several occasions on the Open Government Initiative and on transparency. And we are, indeed, working very diligently on that with our FOIA group and disclosure group.

The FOIA requests themselves are coming in at a faster rate than they did even in FY '09. For the past two fiscal years we have averaged exactly 109,000 FOIA requests. Not exactly, but averaged 109,000 FOIA requests two years in a row.

This year, we have received over, just over 73,000 requests since October 1st. At this time last year, we had received about 60,000 FOIA requests. So we are indeed increasing this. It's a 23 percent increase in FOIA requests.

Despite that increase, we are also continuing to work diligently to reduce our backlog. As of April 2010, the DHS backlog is down to approximately 12,500 requests.

We need to continue to focus on that given the increase and given the uptick. With that said, we are moving in all good haste and apparently, Health and Human Services now has the largest backlog, DHS no longer does. So that's very good news for us. But I'm not competitive in any way.

We also are working on the Open Government

Directive, Initiative as the Secretary mentioned. The Department has made significant enhancements to its online FOIA reading room, as well as posting new information. And that has emerged significantly to our benefit as we are receiving requests and are able to immediately refer them to information that is already publically available.

For example, in the spirit of the Open Government Initiative, DHS has also opted to post all of its Annual FOIA Reports from Fiscal Year 2007 to the present in machine-readable format, as well as in PDF or forms traditionally available for this use.

We are also working on possibly providing our FOIA logs as one of the extracts or elements for the Data.gov initiative, provided, it's consistent with privacy protections.

But again, consistent with the transparency initiative, we wanted to make sure that the information would be out and available for those in the public in order to make sure that we have an open and transparent government.

With that said, Mr. Chairman, that does

conclude my remarks.

MR. PURCELL: Thank you very much. I wanted to rewind a little bit here because you mentioned training in at least three different contexts.

MS. CALLAHAN: Yes.

MR. PURCELL: Not so much a question Mary Ellen, but more of a request for the next meeting. I would love to have an overview of the training. Just one comprehensive overview that says, not only here are the materials that we've produced, but also here are some metrics around how many people.

Whether it's fusion centers, internal component staff, overseas staff, I don't know somebody else. I'd like to kind of understand what that means.

And if it's possible for the Committee Members to review any of the materials, I think that would be helpful for us just to get a better grip on how to contextualize the training effort that you're undertaking here, which seems robust. But it's a little fragmented in my mind, I'd just like to piece it together.

MS. CALLAHAN: Okay, no great. That's a great suggestion in terms of an overview of the training. In your Section 803 report that you received prior to coming here, it has numbers.

MR. PURCELL: Yeah.

MS. CALLAHAN: But we'll try to do is try to put what's behind those numbers.

MR. PURCELL: That would be helpful.

MS. CALLAHAN: Yeah, no I think that's a great idea. And I will kind of caveat that the training is evolutionary, in terms of what we're doing for Department employees.

As the Secretary mentioned, all employees are required to undergo annual privacy training. But also, for the training that Ken Hunt, and Lyn Parker, and Martha Landesberg have been leading related to the fusion centers as well.

MR. PURCELL: Right.

MS. CALLAHAN: But I think laying that out, I think that's a great suggestion and we'll take it.

MR. PURCELL: Education should be forever, that's good.

MS. CALLAHAN: Right.

MR. HERATH: To follow on, that was a great question Richard. So not only the education which would be fundamental, but metrics and then its effectiveness if you have created such a scheme as so. And how many investigations have you had around breaches in policy which would inherently tell you whether or not you're effective or not.

Incidents and those typically are also indications. So that would be -- so a dovetailing of the effectiveness along with that would be wonderful. That was the crux of a lot of my -- my kind of questions to myself.

MS. CALLAHAN: Metrics are not as evolved as the underlying numbers.

MR. HERATH: Well metrics aren't evolved --

MS. CALLAHAN: But I hear you.

MR. HERATH: Metrics aren't evolved anywhere really. But you can sort of -- you know you can tell graphically usually. I mean your incidents will be driven by people's -- because usually incidents, quite frankly, are not intentional, they're stupid things.

People behaving because they don't know what the policies are. At least that's been my experience, at least internally. I mean there's always people trying to attack you. But the internal stuff, which is the people you're trying to educate should be the ones that are behaving well.

And you know, over a period of time you can generally see your -- as you're training -- you know, as your population training goes up and its effectiveness increases your level of sort of stupid things as well as maybe even intentional things will tend to go down.

MS. CALLAHAN: Right, and for metrics, for incidents we do have those numbers. So we will try to find a good way to present them to you.

MR. PURCELL: Great, looking forward to it. Members, anything else?

MS. CALLAHAN: And I did want to say, I appreciated John's suggestion in terms of using educational technologies and tools. And I will talk to Under Secretary O'Toole about that as well. Because I am a big fan of leveraging, training, and figuring out how to do training in the most effective and efficient way. So thank you for that idea.

MR. PURCELL: John are you --

MR. SABO: Quick question.

MR. PURCELL: Mr. Sabo.

MR. SABO: My constant complaint is that you know, the data moves around at you know, terabyte speed or whatever if you add it all together and, you know, the policies are done at manual speed. So one comment on picking up on the prior two comments.

Our metrics are also are a building block towards accountability. And you know I know in the private sector a lot of -- I'll just say my company and some other companies, certain violations mean immediate termination.

MS. CALLAHAN: Mmm-hmm.

MR. SABO: I realize in the Federal Government that's not as easy to do for a variety of reasons. But are you -- have you surveyed as to whether or not, for example, in performance plans of at least the supervisory chain, privacy compliance against their responsibilities is sort of a performance indicator that they're judged on, even if it's a small factor?

Do you have any sense of -- obviously in your office that probably is a key component. But I know a lot of employee behavior is driven by incentives. And one of the incentives is either good you know, rewards or maybe not rewards if you don't do the right thing.

So I wonder if your staff has looked into that or if that maybe an area that you take a look at in the future?

MS. CALLAHAN: So a couple of different thoughts on that. There are two things that I mentioned in my testimony that I want to tease out a little bit.

One is, the reviews that I'm working on with the Compliance Office, or the Compliance -- are you an office? What are you? With Becky and everybody else. A team, they're a team, the Compliance Team. That is, how do we judge how effective are the programs, policies, procedures, PIAs, SORNs, that we put in.

And you know, one of my responsibilities is to engage in a review of basically anything I want in the Department. But I need to leverage my resources appropriately. And one way of doing that is to look at the PIAs, are they indeed being complied with. Is there training taking place? Do people understand what that is?

Now there is, of course, the work that GAO does that Jim talked about, and the work that the Inspector General does. And I'm not trying to duplicate that. But what I want to do is to make sure that privacy protections that are built into systems are indeed retained in the systems one year out, two years out, something like that.

That is something that the office has never done before. And so that is fledgling. We are developing that and we will probably talk about that in September. So that's one way to address what you were talking about John.

The other way, in terms of information and information flow, is this business case that I referenced earlier where we're working with the CIO, with the Screening Coordination Office, with General Counsel, with Intelligence and Analysis, for how to engage in effective and appropriate information sharing.

And how to make sure that the rules, roles, access controls are built into the system, right? So that we can go and define where the terabytes go and who gets to see them.

But at the same time, you have audit and accountability prospects on the back end. But it can't just be audit and accountability. Because once the data's left, and once it's been inappropriately accessed, then that's the privacy violation right there.

So that infrastructure that we're developing is -- would have to go across components and also potentially across different levels from the secret level and different domains. So it's a difficult process but I think from an intellectual and structural perspective, we've made a lot of headway.

But that's exactly what I think you were talking about was embedding the privacy -- the privacy standards and processes, and even the system of record notices themselves, into the structure. So that we can say, yes you can access that, no you can't and have that turned on. And that's not just policy, and that's not just training, but that's implementing what we have as policy and training.

And then the last point I just wanted to mention on HR in terms of reviewing people and not reviewing people. That -- the government is, as we all know, quite Byzantine with regard to Human Resources.

And so I review the people in the Privacy Office, and I don't review other people in terms of what they do and they don't. So that I don't think is something that would be appropriate or fair for me to do.

And at the same time, you know I have a lot of allies throughout the Department including, not just the Secretary, but the -- you know, the CIO, and the Under Secretary for Management, and the Assistant Secretary for Policy. All of whom kind of you know, are my eyes and ears out there as well even if I'm not the one doing the actual evaluation.

MR. PURCELL: Thank you. And last question, Mr. Pattinson.

MR. PATTINSON: Thank you Mr. Chairman. A couple of things, I think, all under the umbrella of identity management. Many of the programs that you're embarking on or will replace involve identity management, which has brought a great deal of interest around privacy and managing that attribute.

The E-Verify program today is operational, running as it is. We see this potential new legislation for immigration reform taking on biometric Social Security cards which may have impact into E-Verify, it may augment it, it may replace it, or it may never happen.

Either way, I think there's a possibility of tasking this Committee with the joint experts that we have to look at something like that as far as the impact and to ensure that, you know, privacy is baked into that potential program.

Secondly, we're going to hear from Ely Kahn later this afternoon on the National Strategy for Secure Online Transactions. I, you know, raise my hand - I'm fortunate to be a reviewer of that already.

And I think this Committee would benefit from having a tasking in relation to that.

Because it really -- if that strategy goes where it's going, I truly believe it has one of the biggest ever impacts we'll see in our society for trusting identity and creating a trusted environment on the internet. So how we actually overcome the challenge of presenting our credentials in the virtual world, not just in the real world.

I mean we have enough problems with cards and whatever, and driver's licenses and real I.D.'s in the real world, but in the virtual world I believe the strategy has a major impact coming our way and I think a very positive one.

And again, I think this Committee has joint expertise, we could look into that in some way to help augment the good work that's already going on. I know it's on a fast track but I'm sure this Committee can step up to fast tracks. That's just a couple of tasking --

MR. PURCELL: We have a rich history of fast track.

MS. CALLAHAN: Well thank you, Neville. And I was going to say that, you know, in terms of identity management, that Ely's discussion of the NSOTS, as we call it, which is a really horrible acronym. It's like the worst acronym I've said to you guys, and I've said some bad ones.

So I think that that -- the identity management concept I think is pervasive in, I would argue in private sector and in public sector life alike. And let's think about how to best utilize the skills of the Committee.

MR. PURCELL: Thank you Mary Ellen. As always, a pleasure to hear from you. Thank you for your very comprehensive update. We look forward to hearing from you again at our next meeting and in between then as well.

MS. CALLAHAN: Thank you.

MR. PURCELL: Thanks very much. We'll take a 15 minute break at this time. We have three presentations of 30 minutes each following the break, plus 30 minutes for the public comments.

So we'll take a break and actually we're four minutes ahead of schedule but we'll go right to 2:00 to reconvene. Thank you very much.

(Whereupon, at 1:40 p.m., a brief recess was taken.)

(Whereupon, at 2:00 p.m., the meeting resumed.)

MR. PURCELL: Thank you, we'd like to begin again. Thank you very much. Our next speaker is Helen Goff Foster, who we haven't heard from before and that's because Helen joined the Privacy Office at DHS as a Senior Privacy Analyst just this last December.

Ms. Foster's planning on briefing us about the developments in the Information Sharing Governance within the Department of Homeland Security.

Prior to joining the Privacy Office Ms. Foster was in private law practice with Washington law firms, both WilmerHale and Bryan Cave, and counseled major internet, communications, and financial services providers on data privacy and consumer protection compliance issues.

She's also served as a Senior Staff Attorney at the Federal Trade Commission in the Division of Financial Practices, where she led some of the agency's first rule making under the FCRA and FACTA, and was a founding member of the Identity Theft program at the Federal Trade Commission.

Ms. Foster, you may proceed.

STATEMENT OF HELEN GOFF FOSTER, SENIOR PRIVACY ANALYST, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, PRIVACY OFFICE

MS. FOSTER: Thank you, Mr. Chairman, Members of the Committee. I am so glad to be here speaking on what I hope is the first of many occasions and to be addressing such an important topic as information sharing governance at DHS.

I don't think there's any question that information sharing is vitally important to DHS's mission. We've all seen examples in recent weeks and months where getting the right information to the right people at the right time has made the difference or can make the difference between effective law enforcement or counter-terrorism efforts and potential disaster.

But getting information sharing right, that is sharing the information in a way that protects that information and ensures that privacy and civil liberties are appropriately maintained, is an enterprise that is rife with complexity. I don't have to tell you that, nobody knows that better than this Committee.

One year ago this Committee issued a White Paper addressing these complexities in the context of information sharing arrangements at DHS and the processes surrounding the implementation of information sharing agreements.

Today, almost a year to the day later, I am pleased to report that DHS has implemented a three prong process for managing the information sharing agreement life cycle that addresses many of this Committee's specific recommendations. And also represents the backbone of a Department wide and consistent approach to information sharing agreements at DHS.

As someone who has been actively participating in these developments as they've been occurring, I am very pleased to report, from my first hand knowledge, that the Committee's White Paper provided invaluable guidance and practical direction to ensuring that privacy and civil liberties analysis and objectives were built into the entire process of managing information sharing agreements. And I'm going to go through that in some detail in just a minute.

But as a starting point, I thought it might be helpful to review the overall information sharing governance structure at DHS. As you may know, information sharing policy and governance at the Agency flows from two interrelated bodies, the Information Sharing Governance Board and the Information Sharing Coordinating Council. The ISGB and ISCC, respectively.

The Governance Board, the ISGB, is the executive level steering committee that sets information sharing policy and provides advice to the Secretary and the Deputy Secretary on information sharing issues.

It consists of the head of each of the DHS components as well as the senior members of the various HQ offices including, of course, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties. This group is chaired by the Under Secretary for Intelligence and Analysis.

Under that body is the Information Sharing Coordinating Council, or the ISCC, which is the working level body that develops guidance and policy recommendations for the ISGB's consideration. It is made up of senior staff members from each of the DHS components. I am a representative of the Privacy Office to the ISCC along with Ken Hunt from the Privacy Office.

Importantly, these two bodies have been in place for some time, but recently there has been a management directive that will codify their respective roles and responsibilities as it relates to information sharing and information sharing agreements and guidance. And we'll talk a little bit about what that has meant right now.

The Information Sharing Coordinating Council, as I mentioned, has implemented a three prong approach to information sharing agreements and managing them at DHS. Step one is the Data Access Request process, or DAR. The DAR is a request for information questionnaire.

It represents a written request for information that is to be filled out by the external party that is requesting DHS information. So that's usually a Federal, State, or local -- Federal, State, local, or tribal partner.

The DAR request specific information about data sets and uses, numbers of users and things of that nature. The completed DARs are then reviewed by a Tiger Team consisting of representatives of the Office of the General Counsel, the Privacy Office, the Office of Civil Rights and Civil Liberties, and the Component data stewards for the data sets that are implicated.

The purpose of this review is to determine whether and how the information sharing request can go forward. Specifically, that group is going to look at whether the request for information, including the intended uses, are within DHS authorities and the authorities of the requestor;

whether the exchange can be conducted in compliance with applicable legal and policy obligations including, of course, system of record notices; whether the exchange can be implemented under an existing agreement or an existing exchange; what specific privacy and civil liberties concerns must be addressed and what safeguards implemented if the exchange is to go forward; and what additional privacy compliance measure should be undertaken, for example, a privacy threshold analysis or a privacy impact assessment.

So once the DAR has been reviewed, and assuming that the result is that the information exchange can go forward, that result and any accompanying guidance from the DAR review process is communicated back to the requestor and to the DHS point of contact for the exchange.

Those parties can then move forward into developing into a formal Information Sharing Agreement, which brings us to step two, the revised Information Sharing Access Agreement Guidebook and

Templates.

The Guidebook is intended to be a comprehensive guide to developing DHS information sharing agreements. It includes a template, which is model language and agreement clauses for both internal information sharing arrangements between DHS components as well as information sharing agreements with external partners.

Under the management directive that I mentioned a moment ago, the Information Sharing Coordinating Council members are responsible to ensure that information sharing agreements align with this guidance prior to execution.

The management directive also requires concurrence by ISCC members prior to the execution of the agreement or the effectuation of information sharing under the agreement. Should there be disputes in that process, they are referred back through the ISCC to the ISGB for resolution.

Now the significance of the guidance is not so much that it exists, as what it says. It contains specific guidance to address privacy concerns, Including: requiring an appropriate level of detail on the data sets and the intended uses for data exchange; a consistent definition of, and protection of PII, and incorporation of the Federal Information Sharing Environment Privacy Guidelines; implementation of correction and redress mechanisms, as appropriate; reporting of information incidents; management of records to demonstrate compliance with the agreement and compliance or maintenance of records to demonstrate compliance with the agreement and with applicable laws; imposition of appropriate retention periods for the data shared; and the implementation of appropriate training and appropriate support related to the data for the receiving parties.

In addition, the Guidebook incorporates tools to assist users in assembling the types of information that they need in order to write an effective information sharing agreement, and I'll mention just two.

One is the information sharing agreement checklist which is intended to pick up where the DAR process leaves off to help the folks who are assembling these agreements to gather the right level of information about uses, data sets, users, and the like in order to incorporate those kinds of details into the information sharing agreements.

And the second is the previously issued State Department and DHS checklist for international agreements which contains a lot of specific guidance for those types of agreements.

The Guidebook and templates I think are very user friendly and comprehensive. And more importantly they approach information sharing agreements from a consistent, Department wide viewpoint that builds in privacy and civil liberties protections from the ground up.

I can tell you that the Privacy Office was the primary editor for this last round of revisions, and that Ken and I sat with the White Paper and went through the Guidebook piece by piece building in the suggestions and the practical insights that you all had provided in the White Paper for the agreement process.

Once an agreement is drafted and approved through the ISCC as complying with the guidance, it then moves to step three which is the Information Sharing Agreement Repository. The repository is an electronic warehouse for DHS information sharing agreements.

It is searchable by agreement descriptors and the names of the parties as well as the DHS systems. So you can search for a particular data set to find agreements -- all the agreements that relate to that data set.

You can also search for particular terms in the agreement if you wanted to see all the agreements that relate to the Federal information sharing environment. You could search on those types of terms as well as searching for particular parties to an agreement.

The importance of the repository is that it provides a method by which we can determine whether incoming data requests are already met under an existing agreement. It also allows us to develop and access precedents for dealing with particular types of issues or types of requests.

And also, and importantly, it helps us to -- assists us in ongoing compliance reviews for agreements regardless of the age or the origin of the agreement because they're all housed now in one place.

The repository, I understand, is about 80 percent complete. They've been backfilling it with older agreements as well as putting new agreements into it. And I have used it and it is a very useful tool.

So in conclusion, I will just say that in the year since the Committee issued its White Paper recommending that DHS adopt a consistent, comprehensive approach to information sharing access agreements, the Information Sharing Governance Board and the Information Sharing Coordinating Council have implemented three significant initiatives to address the gaps identified by this Committee.

Collectively, the Data Access Request process, the Information Sharing Agreement Templates and Guidebook, and the Information Sharing Access Agreement Repository form the backbone of a more consistent Department wide approach to information sharing access agreements that addresses privacy and civil liberty concerns and incorporates fair information practice principles and safeguards for personally identifiable information that is being shared with DHS partners.

I would like to end by thanking the Committee for your kind attention today and also, especially, for the Members’ hard work on the Information Sharing Agreement White Paper. I can tell you that I keep a copy, my very dog-eared copy, in my top drawer, and when I'm reviewing an information sharing agreement, which I do as a member of the Information Sharing Coordinating Council, I refer to it frequently to make sure I'm getting it right.

So I thank you for making my job easier and on behalf of the Privacy department, or the Privacy Office. And I will take any questions that you have.

MR. PURCELL: Ms. Foster, thank you very much. You are setting a dangerous precedent in that our work is actually being implemented in the office.

[Laughter.]

MR. PURCELL: So I think we have to --

MS. CALLAHAN: You know I heard that, right?

[Laughter.]

MS. CALLAHAN: I'm right here.

MR. PURCELL: Is Mary Ellen here?

[Laughter.]

MR. PURCELL: I wanted to thank you but also to thank the Committee for that hard work. I am aware of the heavy lifting that was involved in that paper and wanted to second your kudos for having -- the Committee having produced it. The members did work very hard on it.

I want to turn first my attention to the Guidebook. I haven't seen a copy of the Guidebook. And perhaps the Committee Members would have an interest in reviewing that if possible.

So if it's possible at all to share that with the Committee Members I believe that Members would be -- have an interest in helping substantiate -- substantially confirm our library for the kind of follow-up work. Much like my question earlier on training did. We'd like to peer as deeply as we can into the processes. Not so much as to critique them, but rather just to be more aware.

MS. FOSTER: And I should have mentioned that the status of the Guidebook and the DAR is that they are finished as far as the Committee is concerned, but they haven't been formally promulgated yet. So when they are, we'll work on that and --

MR. PURCELL: At your timing I would love to see a copy of that and I'm sure the Members join me in that. Board questions?

Mr. Pattinson.

MR. PATTINSON: Thank you. Helen, very interesting - thank you for your update. I have a couple of questions. I guess this is one area where the information sharing is subject to that balance of security versus privacy. The urgency for data sharing can sometimes be under mission pressure, et cetera, et cetera.

Can you give me an idea of the time it takes from one of these requests to be put in to the making sure all the checks and balances and everything has been done so that then the grant is provided and the access is then done.

And secondly, or the second part of the question, just to double up my questions, what is the audit that is then going to now be prevalent on the process of now granted and the information sharing's done. What's the follow-up to make sure that it's being complied with?

MS. FOSTER: Great questions and I'll be happy to answer. The timing to approving an information sharing arrangement is really going to depend on what the information is, and the parties involved, and what the purposes are. And because this process that I've just described is just being rolled out, I can't tell you that it's much faster now then it was before.

What I can tell you is that in systematizing the process the way the Agency has, we've really met some very important goals that should make the process both more accountable, as you mentioned, and also quicker.

And that is by systematizing it the way we have, the Privacy Office, Civil Liberties, the Office of the General Counsel, are getting kind of three bites at this apple. When the request comes in, we're reviewing the request and providing guidance there.

We've provided significant guidance in the Guidebook. I mean I think you could title the guidebook “How to Implement Privacy,” rather than just how to implement information sharing agreements generally and you wouldn't be too far off. So we kind of get our hit there.

And then of course, we have the review at the end stage when the agreement is about to be signed to make sure that what we have suggested throughout the process has been properly implemented.

I've seen that take a week or it can take longer depending on what the issues are and how well the folks who are working on this agreement have, you know, been able to digest the guidance and put it into practice.

The caveat is always that, you know, every agreement is different, the issues are always different depending on what the uses are and what the data sets are, whether we've been down that road before with another partner or haven't. And so the process -- and frankly, how important the agreement is at the Agency -- everybody works on their own priorities.

So but in terms of what the system -- what this system has done is it's made sure that we get -- the privacy issues get on the table early and consistently. It also makes sure that the decisions, when there are decisions to be made, are elevated appropriately.

So that once Privacy has made its -- or Civil Liberties and others have made their concerns known, if there is a dispute it gets put back up the chain so that the decision makers are the ones making the decisions.

And the third thing is that agreements do not end up languishing for want of leadership because there is a process through which they are intended to be pushed through. I do know that the information sharing coordination -- Information Sharing and Collaboration Branch at DHS -- is thinking that they are going to start tracking how long it takes agreements to come through the process. So we might have more information on that as we move along.

To the second point of your question, the accountability stage. I know that the Privacy Office certainly does engage in compliance reviews of information sharing agreements. I know of reviews that have happened and I know of reviews that are planned to happen. So that is ongoing as well.

MR. PURCELL: Thank you.

David.

MR. HOFFMAN: Ms. Foster, thank you very much for coming here. I'm greatly pleased to see all of the progress in this area. So thank you again both from me and the Committee.

I may have missed this in the way you were describing the controls that are put in place. Because I went back and was looking at the document that we wrote. And there's been a lot of work that's been being done in the privacy arena since we wrote the document to try to define what the fair information principle of accountability means.

And it was interesting to come back to this document. And I think we captured a lot of what people are defining as accountable organizations. In the document in the questions that we were defining should be asked as part of the threshold analysis to determine.

And so what I'm hoping that you could talk to is, what I took away from your remarks was a tremendous amount of fantastic processes that's being put in place to make sure that the agreements are put in place and that agreements are driven from a general template.

What I wasn't sure, what I'm taking away was, whether there was analysis up front happening about whether the person or the entity that would be being shared with, actually had the requisite controls and whether they actually would be able to fulfill the agreement.

We had -- several of us as authors of the document had concerns when we were originally writing it saying, if this just about making sure that contracts are signed, often times in our experience as putting together compliance programs in the private sector, we know that our vendors, their lawyers will sign contracts, it doesn't necessarily mean that the people who actually own the operational part of it have ever even reviewed that document.

So I was just wondering if you could talk a little bit to the degree to which some of the questions that are asked as components of the threshold analysis might be implemented.

MS. FOSTER: It's a great question and I could spend a significant amount of time on it. I think this is a place where the White Paper continues to be really, really valuable day to day. Many of the types of questions that you're referring to are specifically called out in the Data Access Request process.

So it's something that DHS asks the requestor, you know, what are your controls? How are you doing your information security, things of that nature. And/or, it is something that when the DAR group reviews those requests, those are the questions that we are asking when we're looking at those requests of, you know, who is this partner and, you know, what are their controls in place.

Now a lot of the agreements that we have been working with and I was working with when we were writing the guidance were Federal partners. So you have different types of concerns than when you're dealing with State, local, and tribal partners.

But those types of questions that you're referring to, in terms of digging deep into whether or not this partner can actually implement the agreement, is part of the Data Access Request process.

It's also one of the reasons that we stay -- we want to keep the component data stewards in the loop. And that's why they're part of the Data Access Request review process as well.

Because they are the folks on the ground who are going to be able to tell us, you know, is this information that this requestor is seeking actually valuable for the purpose for which they intend to use it. Because the folks who know the data are the folks who collect it and who are storing it.

And also, is, you know, will the technical requirements be able to be met. Because they are going to have done some research in order to respond to the Data Access Request form in order to make sure that that's actually going to work.

So we continue to use the White Paper and those questions when we review the Data Access Request, when the agreement's being negotiated, when we do the final review of the agreement, we're asking those questions. And then if there's a privacy impact or a threshold analysis, those issues come up again.

MR. HOFFMAN: And has that been systemized so that there are a standard set of questions that are asked or is it more ad-hoc then that?

MS. FOSTER: No, the Data Access Request form is a standard set of questions that apply to everybody. But as you can imagine, when you start talking about specific types of information sharing requests, it can get very detailed and very request specific very quickly.

So the Data Access Request form lays out the broad questions that we want to ask everybody. And then the review process, the people who are in that review process, like the representatives of the Privacy Office, ask the detailed questions that are specific to the data sets with the guidance of the component and the component privacy officers to help us make sure we're headed in the right direction.

MR. HOFFMAN: Thank you very much.

MR. PURCELL: Thank you.

And Jim please, last question.

MR. HARPER: Thank you very much being here. Thanks for your kind words about our work, we're very gratified to hear it.

I didn't bring a copy of the book with me to give you today. But I wrote a chapter -- co-authored a chapter with Jeff Jonas in O'Reilly's recent Open Government book where we talked in fairly abstract terms about data tethering.

The idea that to keep data current among recipients you might use some metadata attached to the substantive data saying where it came from so that there could even be periodic updates when the information changes. All toward the end of having good information allows good decisions to happen using relevant data.

I don't know much about the actual

application of that and I'm just curious to know, is it part of the conversation to start having data sharing that includes routine, real time perhaps updating and that kind of thing. Where is that in the real practical implementation side of things?

MS. FOSTER: Well everybody is interested, particularly in the -- when you're in the law enforcement or counter-terrorism context, everybody interested in accuracy and making sure that the information is the most up to date and is real time and is right there.

So that is -- that's a concern that kind of -- it cuts both ways. The folks who want the data are concerned about that, and as data stewards and data providers, we're concerned that, you know, if we've made errors or there's errors in the data, that those get updated.

But because we're limited by the technology, not only our own technology, but often the technology that exists where we're sending the data, you know it's not always something that right now can be implemented. But as we're looking at things like the information sharing architecture, those are discussions that are being had.

I can tell you that one of the important things that we thought about when doing the templates and the guidance, was to make sure that, you know, absent that type of technology that we are requiring our partners to keep track of where the data's coming -- the data that they're getting is coming from, how they're using it so that we can go back and audit their compliance with our agreements.

And so that is kind of the first step in utilizing what you're talking about, which is more of a utopia of, you know, being able to ensure compliance with promises that are in the agreement.

MR. PURCELL: Ms. Foster, thank you very much for your comments today I appreciate it.

Before we turn to our next speaker, I wanted to -- I'm remiss in not having reminded the room that those who would like to address the Committee after the speakers have made their presentations, there's still time to sign up. The sign-up table is outside this room. Please do so in order to provide your public comments to the Committee.

I'd like now to turn to a familiar face. Lyn Rahilly is the Privacy Officer for the U.S. Immigration and Customs Enforcement component of DHS, with the friendly name of ICE.

Ms. Rahilly implements these policies, procedures, initiatives, et cetera that foster public trust in ICE by protecting personal privacy and enhancing the quality of personal data held by the Agency.

Her responsibilities include ICE's compliance with Federal privacy laws, for training in privacy, for ensuring information sharing policies and agreements that provide appropriate protections for personal information.

Prior to her position as Privacy Officer at ICE, Ms. Rahilly served as Privacy and Civil Liberties Officer and Special Assistant to the Director for the U.S. Terrorist Screening Center, and as Deputy Privacy Officer and Assistant Chief Counsel for the Transportation Security Administration.

Ms. Rahilly, a pleasure seeing you again.

MS. RAHILLY: Thank you.

MR. PURCELL: Please proceed.

MS. RAHILLY: Thank you very much.

STATEMENT OF LYN RAHILLY, PRIVACY OFFICER, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

MS. RAHILLY: Thank you very much for the invitation to speak today. I'd like to give you a little bit of background on ICE as an agency, talk to you a bit about the types of records we maintain as a result of our mission.

And then speak to you specifically about the Privacy Office at ICE, how it came to exist, what we've been doing for the past several years we've been in existence, and some of our accomplishments to date. And then I'd be happy to take any questions that you may have.

Can everyone hear me okay?

MR. PURCELL: That's better.

MS. RAHILLY: Okay, sorry about that.

AUDIENCE MEMBER: If they move the --

MS. RAHILLY: Should I do a sound check?

MR. PURCELL: That's better.

MS. RAHILLY: U.S. Immigration and Customs Enforcement, ICE, is the largest investigative agency within DHS and the second largest within the Federal Government behind only the FBI. We were formed in 2003 as part of the Federal Government's response to the 9/11 attacks, of course through the Homeland Security Act.

Our mission is to protect the security of the American people and the homeland by vigilantly enforcing the Nation's immigration and customs laws. As you probably know, we were formed by taking part of the Immigration and Naturalization Service from the Department of Justice and part of the U.S. Customs Service from the Department of Treasury and merging those together to form ICE.

We have more than 19,000 employees in over 400 offices in the United States and around the world. ICE plays a vital role in the DHS layered defense approach to protecting the nation by performing several functions.

First, ICE protects national security

through the work of our special agents who target, investigate, and dismantle criminal organizations and terrorist networks that exploit weaknesses in our legitimate trade, travel, and financial systems.

Our criminal priorities include counter-terrorism and counter-proliferation and also involve the targeting of intellectual property; child sex touris;, alien, narcotics, weapon, and bulk cash smuggling; human trafficking; immigration fraud; and illegal employment offenses.

ICE also enforces immigration laws to secure the homeland and protect our communities by identifying and removing aliens who support terrorism, identifying and removing criminal aliens, alien gang members, and human rights violators.

ICE arrests and detains these aliens, provides them medical care while in our custody, litigates removal actions of aliens before the U.S. Immigration Courts, and actually removes the aliens to their home countries.

The types of records that we maintain in support of all of these functions are varied, as you can imagine. The mission if ICE is incredibly broad. In all, there are over 400 different laws that through our border enforcement authorities we are authorized to enforce in the criminal realm if they affect trans-border activities.

We obviously have a case management system that supports our case management needs for our criminal investigations. We also have a case management function that is specific to our attorneys who are in the field litigating alien removal cases before U.S. Immigration Courts.

We also have a very large system that helps us process aliens that we arrest, detain, and remove for violations of the Immigration and Naturalization Act. We also have various systems and paper records that support our provision of medical care to aliens who are in our custody and detention, in civil detention.

We also operate some programs you may not be aware of. The Student and Exchange Visitor Program is responsible for tracking and overseeing compliance of non-immigrant student and exchange visitors in the

U.S. And the database that provides that function is called SEVIS.

We also have a law enforcement intelligence branch that does a variety of production of intelligence products to help support our law enforcement activities. That branch is not part of the intelligence community. It is limited to what we call law enforcement intelligence only, not 12333 intelligence such as what's done in the CIA.

We also have an Office of International Affairs and ICE attachés that are stationed around the world at our embassies and consulates. And through our Office of International Affairs we operate a VISA security program that supports the State Department's Consular Affairs Offices in their responsibilities in adjudicating and making decisions on VISA applications to the United States.

And finally, of course like every other agency in the government, a very important set of records that we maintain are records about our own employees and their work in the Agency. We also happen to have records about some of our employees’ family members, as our employees are frequently relocated within the U.S. and around the world. And certain information about family members is collected and maintained as well.

So my office was created in April of 2008 as a result of then Secretary Chertoff's direction to the component leaders to create Privacy Offices in some of the key components. In total, we currently have a staffing set of five positions, including myself, four of which are filled. I have one vacancy that's pending and I'm hoping to fill it this fiscal year.

We obtain our funding through taking money away from other component offices within the Agency. So you can imagine that makes us extremely popular at budget time. That's called a service wide, and various functions that really do cross all parts of the Agency are funded in this manner at ICE.

Finally, we recently concluded, with the Office of Inspector General, an audit that they are performing on ICE, specifically focusing on privacy. And I expect that that audit will be finalized soon and published this year. So you may want to look out for that.

Obviously when we first started, ICE had not had a Privacy Office. The privacy functions were scattered and sort of being picked up on an other duties as assigned basis by a variety folks from our legal division and our IT division.

When I first joined ICE they had only published five Privacy Impact Assessments in five years. So there was quite a lot to focus on when I joined in April 2008. But one of the first things we did was try to establish a means to communicate within the Agency with the offices and employees.

We set up a Privacy Office intranet website where we immediately started to put basic information that would help people comply with some of the legal requirements. We had obviously the various templates that the DHS Privacy Office uses and the guidance. We also created some flow charts for the folks who would be doing PTAs, and PIAs, and SORNs, so they could better understand the process that these documents needed to go through in order to get finalized and approved.

We've enhanced the content of that website over the past two years. We now have additional content, such as frequently asked questions that are intended to address, obviously frequently asked questions that employees may have in a variety of areas.

One of the fastest growing sections in our FAQs has to do with disclosure advice that we get from various corners of the Agency asking, in this situation may I or may I not disclose this information. We've also focused on privacy training and I'll talk a little bit more about that later on.

I wanted to just set the stage for you. When I joined ICE I did have experience doing privacy at a couple of other agencies. And it was an interesting challenge, the previous agency I'd been at was the Terrorist Screening Center, which I'm sure you all are familiar with. It obviously has a very important function in maintaining the Terrorist Watch List, but it's an extremely small agency. It had -- or it was a small center. It was within the FBI. It only had 200 to 300 employees and contractors and two data bases.

So this was a very different scale and scope of challenge moving from a situation like that where I knew every data field and every data base and why it was there and how it worked, to an agency that has over 90 IT systems and a much broader scope and mission.

So I wanted to set out a concept of how we were going to proceed once I got oriented at the Agency. And basically I have kind of a set of strategic goals that I'm following, they're broken up by years over the office. It's kind of a five year plan.

The first years, one through three. What I'm focusing on is building the foundation that I feel is necessary for privacy compliance. Obviously, with only five PIAs in place and over 90 systems, I had quite a bit of work to do. So we wanted to focus a great deal on getting those basic privacy compliance documents done, because as we all know, those often will set the policies and standards that everyone must follow.

I also needed to obviously stand up my staff. It was just me and a detailee I had who was working for me from Ohio, for quite a number of months. So getting the authorization and approval to hire staff and getting the numbers right was an important task for me and still is in these early years.

I also wanted to find ways to integrate privacy into existing processes and take advantage of those processes as much as possible so that we could get the most bang for our resource.

Obviously, we focused early on on integrating privacy into our IT system, the system life cycle management process at ICE, also into the review process for Information Sharing Agreements that existed at ICE, and in our existing policy making processes.

Years two to four, I know am in the beginning of year three, we are going to be focusing a lot on privacy training and awareness. This was not the first step that I chose to undertake because when I came to ICE and I realized based on where they were in privacy documents, SORNs, PIAs, I realized it would be very challenging to try to do any across the board training when you can't even tell people which SORNs to go to and what routine uses exist that authorize the way that they do business every day.

So we really felt like we needed to build the foundation before we trained people on how to use these documents to come to the right answer on privacy issues and questions. We are now focusing on training a great deal.

It's a huge priority for us in this fiscal year and next. We've already implemented Agency wide training at the end of last fiscal year. We took advantage of the Department's Culture of Privacy Awareness Course, and we modified it slightly for ICE and implemented that.

We're also working on customized training. It's really going to be targeted to the types of jobs that people in ICE do so that they can better understand what types of issues they're going to face and how to find the right answer on those issues.

We're also looking to integrate into

existing training we have for leadership as well as certain categories of employees such as our attorneys in the field. And we're also, obviously, always looking to enhance privacy resources that we have available online on the intranet, but also to improve our outreach to the public and to our stakeholders.

And our stakeholders in the case of ICE are obviously Congressional Committees that have an interest in our mission or an oversight role. But also we work with a great many non-governmental organizations, or NGOs, who are very interested in our immigration and detention and removal processes.

And I've spoken to them a number of times about privacy issues and we'll continue to engage them so that they're aware of our programs, but also, of some of the laws that they must follow when they are inquiring about aliens who they are concerned about.

Years three through five, which is coming very quickly, what we hope to do is to build on privacy compliance by implementing again this accountability aspect. By implementing what I would provisionally call Privacy Assistance Reviews within the Agency,

where we going to go to a particular program office or field office and, using a standardized checklist, we're going to go through and assess how well they are complying with the SORN that may govern their data or the PIAs that may govern their data. And also look at vulnerabilities we think they may have and suggest recommended improvements.

And the goal is for us to basically do what an auditor like GAO or the IG may do if they came in. But to obviously do it in an internal manner with an eye toward reducing vulnerabilities overall and hopefully helping the program offices understand on a very detailed level where they can improve on privacy issues.

Finally, I'll just speak a little bit about some of the accomplishments that we've had since our inception. Obviously, you know we have done a great deal of work on our training program and that remains a significant goal for the next two years.

We have, I am very happy to say, we have reduced our PIA backlog. When I joined, our backlog percentage was 17 percent completion rate. It's now up to 73 percent. We've published 26 PIAs or PIA updates in two years. And I'm told by the Department, that that's the most significant improvement in PIA score among all of the components.

A couple of PIAs that are significant that you may have heard about or be interested in. We worked closely with CPB on the Electronic Border Search PIA, as our officers and agents are at the border conducting and supporting searches of electronic devices.

We recently, just this past April, published the Online Detainee Locator PIA, which is a very important initiative at ICE in support of our detention reform initiatives. This is basically going to be a searchable online database in order to find an immigration detainee who may be in our custody. It was modeled after the Bureau of Prisons' locator, which some of you may already be familiar with and has been up and running for many years.

And we plan to actually roll the system out next month in June. And this PIA was published in advance form along with an amendment to a SORN. We're currently collecting public comments on the SORN amendment and that closes on the 2nd of June so we're looking forward to reviewing those.

We focused a lot on operationalizing privacy within ICE. Like I said, we've included privacy in a lot of existing processes. We've also created I think some new angles on operationalizing privacy. One of the things we did early on was we created kind of a variation on the Department's PTA, but this was called a Disposition PTA.

And this was intended to be filled out when a system was dispositioning which we actually have happen quite a bit as we modernize a lot of our systems. And the intent of the Disposition PTA is to see what -- you know, what's happening, why is this system going away, what system might be taking over for it. But also to make sure that the data that is coming from the old system is properly disposed of.

And I do worry quite a bit about end of life cycle privacy risks. I don't really see that it's an issue people pay attention to quite as much as those issues that occur earlier in the data life cycle. So that's been a very successful endeavor and I believe the Department's adopted that and used it in other areas as well.

We work a great deal on information sharing agreements. Helen and I work together on those quite a bit. There are a lot of information sharing initiatives out there, I think, in all agencies. And I think Helen's remarks on that accurately represented some of the successes and challenges we have in that area.

We're also very well integrated into our records management process, which would involve records retention schedules and how long we're going to retain certain electronic and paper records. But we also review all forms and surveys that the Department -- or I'm sorry, that ICE creates and maintains so that we can determine whether or not there's an appropriate collection of personally identifiable information.

A couple other areas we're focusing on in terms of privacy compliance. Our SharePoint systems at ICE, I'm sure you're all very familiar with SharePoint. But it's sort of become the new version of the shared drive within government agencies that have adopted it.

And in my opinion, it presents a lot risks. People often times -- you know, there are SharePoint sites popping up all over the place for various offices, units, and programs. And a lot of times, people who are given access to the site don't know what the rules of access for the entire site are.

So I may be given permission to join SharePoint site A, but I don't know who else has permission. Can everybody in the Agency see it? Is it limited access? And I feel that people need to understand kind of where they are in the electronic SharePoint world in order to know whether they're authorized or not authorized to post sensitive, personally identifiable information.

So we've done some work on creating some policies and also some technologies to try to help orient people. And as a result, at ICE now when you go to a SharePoint collaboration site, the site is formatted one of two ways.

In one way the site is authorized to have sensitive PII. The background of the site you'll see is a certain color. And there's a little, sort of watermark, on the background that says, sensitive PII is authorized. On sites that are not authorized to have sensitive PII, it's a different color and it has the banner that says, sensitive PII is not authorized.

There are also other markers that are on the screen that are a little more prominent than the background. And if you click on the privacy policy on the site, it will tell you exactly what kind of site you're in, what you may and may not do.

In addition to that, we also train every site POC, which is basically the site administrator, on all of these protections and protocols, and what their responsibilities are. And then they are responsible for training the users of that site.

So we've done everything we can, I think, to help avoid a privacy incident by helping to give people visual cues and information that will help them know what they can and can't do when they're on these different sites.

Finally, on the issue of accountability which I've heard a lot of people talk about today, I did want to say that we do focus a great deal on remediation of data breaches and we're always looking for ways to try and improve people's understanding. I do think -- I do agree with the person who said they think a lot of these incidents are inadvertent and that they're done out of ignorance of the requirements.

So we work with the employees and their supervisors to make sure they understand where they went wrong. And we are also exploring ways to incorporate privacy and security obligations into supervisor and employee performance work plans at ICE. And that's something we're going to be working on over the next few months.

The last item I'll mention is we, we ourselves have taken advantage of SharePoint to create a Privacy Office Tracking System or POTS, as we like to call them. And it's a rudimentary system that we set up early on when we first set the office up. And that's basically the way we keep records of all the advice we give, all the work we do on PIAs, and SORNs, and records schedules.

And really anything we do in the office is captured in POTS. And it's the first time I've worked in a Privacy Office, or frankly any other office, that's had that kind of record tracking system.

And we've found it an incredibly valuable tool to go back to a matter and advice we gave a year and a half ago and to see exactly what happened, and what advice was given, and what circumstances. And we've shared that technology with a number of other components in the Department who expressed an interest in it.

So that concludes my remarks today. I would be happy to take any questions.

MR. PURCELL: Thank you Ms. Rahilly. We appreciate the input. I had one question. I don't see any other tents up.

Recently, in our last meeting we adopted and produced a paper on redress. And it must -- it occurs to me that ICE, among all of the different DHS components, must have a lot of inquiries. Certainly the Detainee Locator Database is one way to answer some inquiries, you know where is this person.

But there must be additional redress procedures that you either have or desire to have. Could you explain to us how you handle inputs of complaints of handling, of interviews, of you know, potential breaches of protocols, that kind of thing.

MS. RAHILLY: Well I'll mention two things. First, the DHS TRIP program which you're all terribly familiar with. We do have an office within ICE, within our Office of Investigations that works on DHS TRIP complaints specifically.

They'll get tasked by the TRIP office if, for example, the matter is usually a border, a secondary screening at the border where the record that it's hitting off of is a law enforcement record.

ICE will take that matter, we'll work with the law enforcement agency, be it us or ATF, or DEA, and try to resolve it and see if there are any improvements or changes that need to made to that underlying record. So obviously we do participate in that way.

As for the others, the sort of non-travel complaints that we get. Often times those complaints will stem from an allegation of misconduct involving one of our employees. And all allegations of misconduct are referred to our Office of Professional Responsibility, which has a team of law enforcement officers that will investigate those complaints and determine if there's any disciplinary action that may be warranted. Which could include disciplinary action for a violation of our standards involving the handling of personal information.

So often times, because that is a separate process, it can become a criminal inquiry. So we sort of have to negotiate that on a case by case basis. How we may participate in that versus OPR taking the lead. And that's primarily how it's handled.

Of course we do have programs like the Student Exchange Visitor Program I mentioned earlier and that actually -- there they actually have separate processes and procedures that if a Student or Exchange Visitor feels that their information in the system is incorrect.

There's an entire separate set of processes that would govern how they do that. So a lot of our redress procedures may also be case by case, program by program.

MR. PURCELL: And are you monitoring the progress of those, how long it takes to resolve an issue raised?

MS. RAHILLY: No, we're simply not at that point yet. Again, that would be something that I hope when we get into these privacy assistance reviews, we'll really be able to start working with programs on those types of granular issues and seeing if there are ways that they can improve.

MR. PURCELL: Thank you. Members, any other questions?

[No response.]

MR. PURCELL: Thank you very much Lyn, I appreciate your time today.

We'll turn to our next speaker, Ely Kahn. We have a perfectly good podium that's gone unused all day. And so you're welcome to take the podium. Carpe podium if you'd like.

MR. KAHN: I'll sit.

MS. CALLAHAN: We're kind of informal.

MR. PURCELL: It's kind of the podium set for Elijah.

MR. KAHN: I would feel way to official if I stand at the podium.

MR. PURCELL: Our next speaker is Ely Kahn. Ely is the Director for Cybersecurity Policy at the National Security Staff within the White House. In this role, Ely is leading the National Security Staff's efforts in both cybersecurity legislation, online identity assurance, and cybersecurity education and awareness.

He previously has served in two capacities within DHS. First as the Deputy Chief of Staff in the National Protection of Programs Directorate, and also as the Director of Risk Management and Strategic Innovation in the Transportation Security Administration.

Mr. Kahn, welcome.

MR. KAHN: Thank you.

STATEMENT OF ELY KAHN, DIRECTOR FOR CYBERSECURITY POLICY, NATIONAL SECURITY STAFF, THE WHITE HOUSE

MR. KAHN: Thank you for having me here today. So I'm here to talk about our National Strategy for Secure Online Transactions. And this is an effort that's been underway for the last several months.

The driver or impetus for this effort was the President's Cyberspace Policy Review. And in the President's Cyberspace Policy Review there are 10 near term action items. One of those 10 items is the development, calls for the development of a cybersecurity focused identity management division and strategy.

And so we took that requirement inside our interagency process at the White House and created a working group comprised of representatives from across the Federal Government. We have folks from the Federal Trade Commission, Department of Homeland Security, the law enforcement community, even the intelligence community, that began scoping out this requirement under the Cyberspace Policy Review.

And initially we were thinking about calling this the National Strategy for Identity Management, and decided that sounded much too big brotherish. And really the outcome that we're driving towards is more secure online transactions. And so we thought that would be a more appropriate title.

However, I should qualify that,that this document is still in developmental stage. Everything that I'm saying here today is as the document currently stands in its present state.

We just recently closed one of our review periods and received about 2,000 comments on the draft document. And so actually this pile of paper in front of me is some of those comments that I've been feverishly going through in anticipation of a drafting session tomorrow.

So we do expect the strategy to change over time. And so I'll talk about the high level concepts and the strategy and the way that we think it's going to turn out. But it may change over time.

So in addition to the present Cyberspace Policy Review there are, of course, a number of other drivers for why we're developing the strategy. We believe that a stronger identity assurance and identity management systems for online transactions can help reduce fraud.

We've seen a number of examples of that including in Europe and the U.K., where the implementation of multifactor authentication for online banking dropped online fraud from the millions of pounds a month for an average bank to just a few thousands of pounds a month.

And so we believe that through stronger authentication and identification systems for online transactions we can reduce online fraud and help fight cybercrime. We believe that through improved authentication techniques we can actually also improve privacy in addition to improving security.

We reject the notion that security and privacy are a zero sum game. And we're actively looking at processes and technologies that can support both those concepts.

From a customer user experience we believe that through the national promotion of more interoperable and stronger authentication technologies and processes, we can help fight the proliferation of passwords.

So I think we all probably have a post-it note sitting by our computer with a number of user names and passwords. We think we can reduce that problem, which is actually not just a customer experience problem, but also a security problem, through the adoption of improved authentication processes.

And then lastly, the technology agenda for this Administration is broad. And technology is a very important focus of this Administration. You will see millions if not billions of dollars being poured into initiatives such as the Smart Grid, such as Health IT, and electronic health records.

All those -- many of those initiatives require identity solutions. And so we want to utilize this strategy as a platform to search for more interoperable, stronger, more privacy enhancing identity solutions across these various initiatives. So we're hoping the strategy can help break down some of those stove pipes.

The strategy itself is organized like a traditional strategic plan. We have a vision, goals, and objectives. And then we're also having an accompanying action plan that takes those goals and objectives and turns them into more tangible actions that the U.S. Government will take inside its legislative and budgetary processes to make this strategy real.

What I'll quickly do is walk you through the highlights of the strategy as it currently stands with the qualification that it may change. But these are pretty broad topics and really are the foundation for the strategy itself. So I feel pretty comfortable saying that these, you'll see these themes and concepts in the final document.

So the vision and scope. The scope, as I referred to earlier is really on online identification and online authentication mechanisms. What we're envisioning here is an online environment that is grounded on end to end trust. And so we're looking at establishing what we're calling, an Identity Ecosystem where both organizations or individuals on either end of the transaction are strongly identified and authenticated. And the underlying infrastructure that those transactions run on, the servers, routers, those are also strongly identified and authenticated.

We recognize that for online transactions that there are a variety of different types of transactions ranging from transactions that are very sensitive, online banking, filing your taxes, to transactions that require anonymity such as blog posts or logging into various types of websites.

And so in this strategy we recognize the range of transactions and we recognize that there is not a one size fits all solution and that any authentication solutions that we do pursue are risk based and tailored to the authentication requirements for that type of transaction.

So that being said, the scope is broad. It is looking at authentication of not only the individuals or organizations involved in the transaction, but also the devices, or infrastructure involved in that transaction. It builds on a lot of the good existing work that's happening inside the Federal Government.

So some folks may be familiar with the Federal Identity, Credential, and Access Management segment architecture. This is an effort that was undertaken by OMB and GSA to better define how the Federal Government should be rolling out its own authentication and identification technologies for both physical and logical access management.

And essential to that segment architecture is the realization that the government needs to do a better job at figuring out how they can accept third party credentials to log into government websites.

So inside the government there are a number of pilot projects underway where the government is now accepting credentials from third parties. Whether that be a credential provided by Google, or by even Facebook, and using those credentials to log into government websites depending on the authentication requirements for that website.

So we're building on some of the concepts in that segment architecture and expanding on it. So we're not looking at just government to citizen transactions or even government to government transactions in the strategy.

But we're building on that and looking at what are the national policies that we want to try to put in place that build, that encourage stronger authentication protocols for citizen to citizen, citizen to business, business to business type transactions. So in that sense we are looking fairly broadly at different types of solutions that the government can influence.

So moving beyond the vision and scope, in terms of guiding principles, we have four main guiding principles in the strategy as it currently stands. And these guiding principles really undergird all of the recommendations and the goals, and objectives that you see in the strategy. So you'll see these guiding principles interlaced throughout the document.

So the four guiding principles, the first one is that identity solutions should be secure and resilient. And so when we think about identity solutions that are secure and resilient, what we're talking about are identity solutions that are resilient to attack.

So that they should utilize strong cryptography wherever necessary. They should be resilient to accidents. So if an individual loses their credentials, they should be easily revokable and lose-able. They should be resilient to change. So they should be built in a modular fashion that is adaptive to how technology adjusts over time. So they shouldn't become obsolescent with technology changes.

Our next guiding principle is that the identity solution should be voluntary and privacy enhancing. So the voluntary piece is important. We're not talking about implementing a new National I.D. Card. We're talking about creating an environment where citizens have a variety of identity solutions to choose from to improve their ability to authenticate themselves online if they so choose so.

And in terms of privacy enhancing, we often times utilize metaphors from the offline world to talk about the types of privacy features we'd like to see in the online world, in this strategy. So one example that we use in the strategy is the example of a driver's license. So there are good privacy aspects about driver's licenses and bad privacy aspects about driver's licenses.

In terms of good privacy aspects, when I utilize my driver's license at a bar, a bank, movie theater, generally those transactions are unlinkable. There's no real entity that's taking those transactions, aggregating them, and trying to link how I'm using my driver's license across those different sectors. We'd like to try to replicate that same principle of unlinkability in the online world when we're talking about identity solutions.

Now in terms of the bad aspects of driver's licenses. You know when I do use my driver's license at the bar I'm not only revealing the fact that I'm over 21 to the bouncer, but I'm also revealing my home address, my actual date of birth, my height, weight, et cetera.

And that's -- that aspect of driver's license is something we can actually do better about in the online world through principles of data minimization. And so we're actively looking for identity solutions that do better than some aspects of offline driver's license use.

Our next guiding principle is that identity solutions should be cost effective and easy to use. So this is pretty self explanatory. I think a key point though is that one thing that we are trying to do in this national strategy is identify ways that we can make the business case, from a business or industry perspective, more attractive to adopt more interoperable, more privacy enhancing, stronger identity solutions for transactions that need them.

And so there's a number of ways that the U.S. Government can make the business case more attractive to industry or that through -- that can be just raising awareness, it can be through grants, it can be through other market based incentives. So we're taking a hard look at the various levers that are available to government to make that business case more attractive.

And then lastly, our last guiding principle is that we want our identity solutions to be interoperable. And so the example we often use there is the ATM card. The ATM card is built on open standards that allow an individual to utilize his ATM card at any ATM machine around the city, in the country, even internationally. And so we want to look at ways to build that same level of interoperability into our identity solutions wherever possible.

Next, the goals and objectives. And so the goals and objectives, these are the goals and objectives to build our Identity Ecosystem that we're envisioning. And often times we use a very simple metaphor to describe these goals and objectives. We have four goals, and we think about these four goals a lot like building a playground.

And so the first goal is design the blueprints for that playground. And under that goal we're looking at what are the overarching standards that need to be put in place to encourage this interoperable privacy enhancing secure Identity Ecosystem.

We're also looking at what -- if there need to be any legal adjustments or liability adjustments that need to be made via legislation or other means that encourage interoperability and privacy enhancing aspects of this Identity Ecosystem.

The next goal is about building the infrastructure associated with the playground. So building the playgrounds and swing sets, and slides. And so under that goal we're looking at establishing new pilot programs with the State governments and how the Federal Government can support the State governments’ efforts to deploy strong, interoperable privacy enhancing credentials to their citizens.

We're looking at new grant programs that can support those efforts. We're also really emphasizing how the government can be a leader in these efforts so that we're providing a role model and leading by example around strong identity solutions.

And so this is not only, what I mentioned earlier, about building trust frameworks where we are accepting third party credentials, but also looking at how we can better authenticate our infrastructure.

And so making sure that we are rolling out things like DNS-SEC, IP-SEC, e-mail authentication.

You know, various types of authentication protocols related to our infrastructure and be a leader in that sense.

The third goal is about making sure that the students feel safe and that they know how to play in the playground once it's designed. And so in that sense, under this third goal we're talking about creating education awareness programs for the American public and also for industry about strong interoperable privacy enhancing identity solutions.

Probably, most importantly also under this goal three, we're talking -- we have a number of recommendations around improving privacy protections for the players within this Identity Ecosystem. More specifically, we're looking at how we can adopt the Fair Information Practice Principles for various players within this Identity Ecosystem.

We have a number of very smart privacy folks on the team, a few of them sitting behind me today who have been helping us in -- I would say that this is probably one of the more break through areas of the strategy as we look at the Fair Information Practice

Principles and how the U.S. Government can more strongly support those in this Identity Ecosystem.

Under the last goal, goal four, we're talking about how we should manage this playground to ensure its long term success in the future. And so we have a number of sort of longer term initiatives including research and development initiatives around strong interoperable identity solutions.

We also discuss how the U.S. Government should be playing in the various international forums. Whether that be international policy forums or international standards organizations to help ensure that the solutions we are developing are interoperable on an international scale whenever possible.

And then lastly, in terms of the internal U.S. Government, government structure, we're looking at various models including the potential for a national program office inside a department or agency to help coordinate the various efforts that we're laying out under the strategy.

So as I mentioned, there are these four goals and a number of objectives under each of these goals. And then under each of the objectives, a number of specific actions. And those actions will be going through various levels of government review, but ultimately, those will translate into new government programs and policies that will help implement the strategy.

So just before I wrap up here, just a few examples and I'll also talk quickly about our time line moving forward. And so it always helps me to think about examples to make some of these concepts more real.

So I'll qualify these examples as, these are illustrative examples, not necessarily things that we are specifically advocating for in the strategy. But I think at least help demonstrate the end state that we're trying to get to.

And so one example is that, perhaps in the future we'll live in a world where we'll all have smart ATM cards or smart health cards. And in those smart ATM cards or smart health cards there will be a chip that contains, in a secure and privacy enhancing way, information about me that I can utilize to authenticate myself, not just to my bank or to my health care agency, but to any other relying party that signs up to utilize the open standards embedded in that chip.

So I'm not sure how many folks here are inside the Federal Government, but I know I wear a war necklace of different I.D.s or credentials around my neck. And I think we're trying to get to a place where instead of that war necklace of I.D.s or credentials, we're giving citizens the option to utilize a smaller number or perhaps even one strong interoperable credential that they can utilize to authenticate themselves in a privacy enhancing -- a privacy secure way to various different relying parties inside and outside of government.

Another example you know, in terms of international use. I'd like to get to a place where if I'm on vacation in say Germany and I break my leg, I'm able to use my health care card in Germany so that my doctor in Germany is able to access my health care information securely from my doctor in the United States. And that my doctor in Germany is able to utilize his credential to authenticate himself to my doctor in the United States to prove that he is indeed a licensed medical professional.

So those are just few examples in terms of you know, the types of interoperability that I think we're trying to get towards through this strategy. And you know, in both those examples we're also striving towards a system where those transactions are running on secure, authenticated infrastructure to prevent them being grabbed on their way to the United States.

So in terms of time line moving forward, I mentioned that we're in the middle of a review process right now, going through quite a number of comments that we've received thus far. We are hoping to push out another version of the document in a much more public fashion in the next 30 to 45 days or so.

And we will plan on using a Web2.0 tool via the whitehouse.gov website to gather comments, generally from the American public on this strategy, with the intent of ultimately finalizing the strategy by the end of the fiscal year and taking a lot of the recommendations and pushing them into the implementation process as soon as possible.

So with that, I'm happy to take any questions and thank you for your time.

MR. PURCELL: Thank you Mr. Kahn. Questions, so many questions. Yes, rather than taking my prerogative, I'll start with the Members.

Howard, please.

MR. BEALES: Thanks. I was -- it seems to me that the heart of identity management system has got to be, and the heart of secure online transactions has got to be a pretty much unbreakable link between the credential and the person.

That means the person can't walk away from it. Because that is sort of the heart of the fraud problem. I invent an identity, it's perfectly fine for awhile. And then when I commit my various bad acts, I abandon it and start a new identity.

That's very hard to square with fair information practices and the notion that users have complete control over what information they're going to provide and to whom. Because the heart of it is the unbreakable link. And so I'm wondering how you're trying to square that circle in this document.

MR. KAHN: So there's a -- it's certainly a tough problem and I think we recognize that the identity solutions that we are abdicating for in this strategy are one piece of a larger solution. And so to create secure online transactions, we need strong identity solutions but there are a number of other pieces of this cybersecurity set that are also required to provide secure online transactions.

So for example, we can have a very highly authenticated individual in a -- that takes place during a transaction using a strong multifactor credential. But if the box, if the computer that that individual is utilizing is compromised, it really doesn't matter how strong that credential is.

And so, you know generally speaking to your question, I think we need to look at not just what the strong identity solutions are that are needed to conduct secure online transactions, but what are the other supporting infrastructure solutions that are needed to complete that puzzle.

MR. PURCELL: Thank you.

Kirk.

MR. HERATH: I appreciate your job. A few years ago my company had sort of a nascent attempt at creating Federal Identity Program, sort of a cooperative. And where we found it breaking down, it was really not around the technology.

Right, so we'll never be able to create a system that's secure completely and affords 100 percent privacy. Where we broke down was on the identification of the sort of reciprocal liabilities that we all enter into when we come into this beast, right?

So you mentioned it in your remarks. I would -- actually my comment really is it's the legal liability policy issues that I think are the key to this whole thing. You know if you have a joint and several liability system, which is what it is unless it's not, right by law, it will devolve into, into chaos and anarchy.

So really, where I finally came down was there needs to be some sort of a no fault -- almost a no fault insurance mechanism that helps people who have been harmed. There will be people who are harmed because humans are going to be the weakest link of the system. You've still got technology interacting with human beings. And I'm talking about the human beings running it, not necessarily the ones who are using it.

So as long as you've got human beings running it, there will be mistakes intentional or otherwise, and people will be harmed. There needs to be a way of taking the harm out of the system, compensating them, figuring out what the root cause was, fixing it. Meanwhile, everything's continuing to flow, right?

And in a nutshell that's -- I think that's the key. I think it's a huge undertaking that'll require a lot -- a lot of changes to the law and to our legal culture.

MR. KAHN: Yeah, I couldn't agree more. It's a particular area of interest for our team. We've been doing research around how other countries have handled the liability issue. There's a number of other countries, European, South American, Asian countries that are -- have also gone down this road.

And in some of those countries there have been explicit liability caps put on identity issuers that have helped spark adoption. And I don't think we can get to broad adoption without some review of existing liability regimes and looking at some adjustments.

MR. PURCELL: Thank you.

Lance.

MR. HOFFMAN: Thank you. Thank you for coming and talking to us today. It's refreshing to get the strategic overview because so often we tend to get bogged down in the details of implementing something. I think it's very forward looking.

What I'm interested in is if you've had a chance to look yet at how you're going to incentivize the various departments of the government to -- not only DHS, but in general, to pilot any of these, to adopt any of these, you've got a whole bunch of interesting issues tied up here.

I think your vision is great, but I'm also, like Kirk, worried about getting bogged down in the details. So strategic plans are nice, but come the end of the year, how are you going to incentivize anybody to do it as opposed to carry on just like they've been doing.

MR. KAHN: I completely agree with the comment that strategic plans are nice, but. And I've been involved with a few other national strategies. And one thing that I wanted to make sure that we did with this strategy is not just have a strategic plan but to have an implementation plan associated with it that went along with the strategic plan to the President when he signs off on the strategic plan.

And so in terms of motivating or incentivizing adoption within government -- actually, I think that will be a little bit easier than incentivizing adoption outside of government. Inside of government, one thing that we are doing right now is relooking at the metrics and compliance requirements associated with the Federal Information Security Management Act.

As we are redoing those metrics, we will be looking at how we can incorporate some of the concepts around identity systems into those metrics. We also, you know, have the power of the White House to try to drive action.

And this is a priority for Howard Schmidt, my boss, the Cybersecurity Coordinator. And so as we're looking at the development of new policy memos and new policy requirements for cybersecurity areas, this will certainly be at the forefront of those issues.

Incentivizing industry is I think a little bit trickier for us in that you know, I think we are very reluctant to look at overly regulatory measures. We are actively searching for more market based incentives.

We're looking at ways we can raise awareness to drive adoption. And we're looking at the government being a role model. Not just in how it structures its infrastructure but also how it leverages its buying power.

And so you know, we are looking at ways in which we can structure requirements into government contracts to require strong interoperable privacy credentials and things along those lines also.

MR. PURCELL: Thank you.

Jim, you're next.

MR. HARPER: Thank you. And thank you for being here Ely. We've talked before. I've been involved in this process and I do mostly want to talk about process. They are doing a really good job of circulating this stuff out.

And if it's all right, I'll recommend to people that -- on this Committee that want to be involved to get your e-mail to Ely so that you can be on the list and see the document in its various stages. Because it's been -- having the opportunity to participate is valuable.

My comments so far have -- I'll say it this way, Ely has very graciously appreciated the comments that I've given because I haven't been terribly satisfied with its -- the document's approach to privacy. And in particular I think talking about privacy as control is important and there's not enough of it in there.

I've said this all to you, I'm sort of

repeating it for the benefit of my colleagues. And the data minimization principle which is acknowledged far along in the document, isn't included in the early part of the -- it's probably just a clerical error, but it's pretty darn important in the identity area to do data minimization.

I very much appreciate using the example of showing I.D. at bars because I'm so practiced in it. But other than -- not for looking young, that's for sure. Other than that though, I do want to -- I just want to commend to my colleagues to participate in this thing.

I don't know that this project will ultimately succeed because it has the characteristics of trying to boil the ocean. But getting people thinking about these things in a good way is a good thing no matter what. So thanks Ely and I just want to make those comments.

MR. KAHN: I'll just react really quickly here. So in terms of providing input to the strategy, we are actively seeking input from folks out in the private sector. Typically, we've been trying to structure input through advisory councils such as this one, or through nonprofit associations.

I believe that there is some conversation with the folks here that oversee the DPIAC structured around how we can formerly get input from the Committee here. So I look forward to that.

The strategy itself is completely dependent on the quality of input that we're getting from folks outside of government as well as inside of government. So I really value the input that we've received so far and it's making the document a much better document.

MR. PURCELL: Neville.

MR. PATTINSON: Ely, nice to see you in person. First of all commending your team and yourself for great work in putting this document out, for allowing us to review it. And as I said before, I am involved in a group that is providing comments back. The liability issue was managed by Kirk.

There needs to be I think a strong understanding that in any identity management environment people have to have a choice of what identity they want to project. With a driver's license we don't get much choice, it's our real identity and real biographical information.

And I've been a long time since talking about the online identity crisis that we have. We don't know how to verify who's who. But we also need to decide who we are when we're in the online environment. And there are times when our role will be such that we want to be identified fully. There will be times where we want to be a different persona and not necessarily completely identified.

So that scale between anonymous to identified needs to be encompassed and I think that's certainly part of the mission that you've got in there. And I think that's important so that people can choose to adopt how they're going to exist in the online world, in that space.

And important to me in looking through the strategy is the certification program for the credentialing providers. How do we make sure they're good and they are doing what they say they're going to do and what we need them to do underpinning this whole credential process. I mean the technology aside, we need to have good strong credential providers and vetting for that.

And just picking up on a comment on how you can involve the Federal Government, and hopefully one of the badges at least around your neck is one of the PIV cards that are going through the program. All Federal employees are now going to be issued that. But there's a great community that can be adopted into this with -- where already a strong credential exists.

So looking forward to the next version and real happy that you've got it back right now because you know it's like two weeks of stress and then kind of a two weeks of rest. So glad you've got it back now. But carry on, terrific job and I'm looking forward to the next version.

MR. KAHN: Thank you.

MR. PURCELL: Charles.

MR. PALMER: Just a plea. You have bitten off quite a bit and my colleagues and I have been involved in other experiences where we've tried to establish --

MR. PURCELL: A little louder.

MR. PALMER: We have been involved in other opportunities to try to get a good credential of one sort or another, whether it was passport or loyalty cards or whatever. And invariably, the consumer -- I'm sorry, the requestor when we approached them and said, gee you really ought to try to get this right and pour every bit of security over it that you can, they said, gee thank you for sharing and chose another path.

I certainly hope that you strive to get the Neville point as well as the can't-be-copied,-can't-be –created-by-other-folks thing correct. Because if you succeed, and I'm sure you think you will, and I hope you will, this is going to be a very valuable target. And if we get it wrong, again, you will have wasted all of your time and we really need to get it right. So good luck.

MR. KAHN: I've had a number of folks that are much more experienced then me joke with me that, I guess we're taking yet another swing at this identity management thing. And so I certainly recognize that there have been numerous attempts to try to solve this problem.

One think I'd say that's different this time around is that we do have the attention of the President, which is fairly unique. I tend to doubt that the President has shown attention in this problem, at least to the depth that he seems to be showing this time around.

And that we have briefed him on this strategy and the progress that we've making on the strategy. And he plans to hold us accountable to delivering on this strategy. So I'm very hopeful that we can utilize the pulpit of the President to drive change.

MR. PURCELL: Joanne.

MS. MCNABB: I have a basic dumb question to which I don't have the answer. I don't quite get who is going to determine who the credential or identity providers are. Is the government role to set standards, or to review and approve?

MR. KAHN: So the government role is not even to set standards. The government role in this case is to participate in standards development activities. So we want these standards to be based on international open standards. So the government will be participating in those efforts --

MS. MCNABB: And the private sector as well?

MR. KAHN: Correct.

MS. MCNABB: But at this point, the private sector isn't involved in this very much?

MR. KAHN: So the private sector is involved in various international standards organizations. And so I'd say if anything, the government hasn't been involved in some of those efforts as much as they should be just because of, more than anything, lack of bench strength.

I think the government will also have a role in incentivizing adoption. And so we hope to create market incentives for people to adopt, organizations to adopt strong privacy enhancing credentials --

MS. MCNABB: But to provide them?

MR. KAHN: -- and so, so it will --

MS. MCNABB: Can you create --

MR. KAHN: -- so it will really be an organic, organically driven, market based effort for these identity providers to stand up.

MS. MCNABB: So why do you think the market hasn't generated that yet?

MR. KAHN: A variety of reasons. It's sort of the classic chicken and / or the egg problem. You know identity providers aren't going to stand up until they know that they have customers. And customers aren't going to buy credentials unless they have places to use them.

And so we're trying to attack that problem from a couple different angles. So that, one, we create incentives for individuals or organizations to adopt credentials. And we create incentives for organizations to adapt their back end infrastructure to accommodate such credentials.

MS. MCNABB: Thanks.

MR. PURCELL: Thank you.

Dan.

MR. CAPRIO: Thanks Ely. I just wanted to echo Lance and Jim's comments and the comments of others and really commend you on the process, the openness and receptivity and the energy that you and some of the others have shown. And rather than repeat some of the points that have already been made, it does strike me that in the process to date, recognizing this is a national strategy, to the extent that we can be helpful and the expertise of the DPIAC, in some ways to add some definition, to operationalize some of the concepts, and Lance is exactly right I think on the notion of pilot projects. But you know, many of us have worked on this for many years. And we want to be, you know, helpful and serve as a resource to you.

MR. KAHN: Yeah, I think interaction with the DPIAC as a whole would be very important. A number of folks on the Committee here have been participating, but I personally would value consensus driven input from the DPIAC. I think that is all that much more powerful. Either in development of the strategy or in helping think through implementation.

MR. PURCELL: Mr. Kahn, thank you very much. We're very interested to continue observing the story of Ely and the search for the Golden Fleece.

[Laughter.]

MR. PURCELL: This has been -- this is a work in progress and we know it will progress in the short term. So thank you very much.

MR. KAHN: Thank you.

MR. PURCELL: We look forward to hearing from you again sometime in the future.

MR. KAHN: I appreciate it.

MR. PURCELL: At this point we would like to take any public comments. We have no sign ups for public comments at this point. Is there anybody in the room who just failed to sign up and is dying to talk to the Committee?

[No response.]

MR. PURCELL: Toby?

[Laughter.]

MR. PURCELL: Perhaps not, shyness. My thanks to all the speakers today. To Mary Ellen, to the Secretary, as well as to all the speakers for their time. It helps us tremendously to receive these inputs and to provide an engagement for questions and answers.

This concludes the public portion of today's meeting. We're grateful for your interest in the Committee's work and we look forward to seeing you soon. The transcripts for this, as well as the minutes of this meeting will be posted on the DHS website, the Privacy Office's website in the near future. And we encourage you to follow our work by checking our web page frequently and we'll set up a Tweet at some point I'm sure.

Would the Members of the Committee please remain for a short administrative session? And we'll ask the public to leave as soon as possible so that we can commence that session.

Thank you very much, meeting adjourned.

[Whereupon, at 3:39 p.m., the meeting was adjourned.]