DEPARTMENT OF HOMELAND SECURITY MEETING
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
FULL COMMITTEE MEETING

SEPTEMBER 17, 2008

Hampton Inn Tropicana and
Southwest Event Center SW
Event Center B
4975 Dean Martin Drive
Las Vegas, Nevada 89118

MORNING SESSION:

MS. RICHARDS: Good morning. So today instead of a stenographer we have a videographer, that's why there's a videotape over there. And then they will be sending it to the stenographer who will then go from there. So, good morning, everybody, this is the opening of the DPIAC meeting. We will – I will turn it over to Howard.

MR. BEALES: Thank you, Becky. Thank you and welcome, everyone, to our public meeting of the Full Advisory Committee today.

A couple of housekeeping items -- please be sure to turn off your cell phones. We will have a ringtone competition at lunch, and you wouldn't want to give away your secrets.

Second item is if you're interested in signing up for public comments, we'd love to hear from you. And please sign up on the table outside the room -- as you came in there.

As is our custom, we will begin with an update from the Privacy Office with Hugo Teufel, who is the Chief Privacy Officer at DHS. He was appointed by Secretary Chertoff in July of 2006 and serves as the Chief Privacy Officer and Chief Freedom of Information Officer. Before joining the Privacy Office, Hugo was the first Associate General Counsel for General Law at DHS, and before that he was the Associate Solicitor for General Law at the Department of the Interior. Hugo, welcome, and we look forward to hearing what's going on.

MR. TEUFEL: I am Hugo Teufel. I am the Chief Privacy Officer at the Department of Homeland Security. It's great to see all of you here today. And all of you who are behind me, especially those from the public who are here –

UNKNOWN: [Speaking off microphone].

MR. TEUFEL: -- I'm very grateful for your attendance. Does that count? I mean, that's equivalent to a ringtone. So it's been awhile since I've been before the Committee as the whole committee. And it seemed like the last two meetings something had come up that precluded my being able to attend. And as we'll discuss during the administrative session at lunch, I thought perhaps that might happen again but I was able to get out here late last night and join you today. So I'm looking forward to today's discussion.

And I understand that you all had some site visits yesterday so you were able to see RFID in action at the airports and visit a fusion center.

In the time that I've got, I want to talk a little bit about what we've been doing in the Privacy Office over the last few months and give you a sense of where we are. And let me start off by saying we have gotten the first draft done of our annual report, and I anticipate that we will have the annual report out probably within the next month or so. I'm looking forward to it. It's probably -- no, it is the best annual report that we've done to date. And you will see a lot of great stuff in there, some of which I will highlight today.

On policy, I want to note that back in February of 2008, we issued a letter to notify Congress of our progress in preparing a comprehensive report pursuant to 804 of the 9/11 Commission Report Act requiring annual reports from the various agencies on the use of data mining. And we acknowledged yet another definition for data mining by Congress -- additional reporting requirements, and we listed the DHS programs that met the new definition. And we indicated that we would be preparing a comprehensive 2008 report in light of the new definitions and reporting criteria. And we're hard at work on that.

Also, and in furtherance of our requirements under Section 804 of the 9/11 Commission Report Act, we held back in July, a data mining workshop that I think some of you attended and was heavily attended by members of the public, the Privacy Advocacy Community and the Department back on July 24th and 25th of this year. So we hope to have that report out soon, probably within the next month or two, and it will be the third such report that we've issued to Congress.

On compliance, which is the next subject I want to talk to you about, we've made some really substantial progress. Over the last year, we've issued 63 Privacy Impact Assessments and 14 System of Records Notices. And as a result of that work -- and that doesn't sound like a lot -- but as a result of that work, for FISMA scoring our numbers have increased on PIA's from 26 to 48 percent, and on Systems of Records Notices we went up from 65 to 90 percent. And 90 percent is a threshold level for FISMA scoring. We made it; it's the first time that we've made it. That's a big deal.

You'll have to forgive me. I'm a little froggy in my throat so I'm relying on green tea.

Speaking of SORN's, something that we started about a year ago is beginning now to take fruit, and that is our Legacy SORN project. As you may know, there are about 270, 280 Systems of Records Notices. These are documents that were required under The Privacy Act of 1974, and they are documents that provide some transparency in notification to the public about the things that the Department and all departments in the executive branch of the Federal Government do with personally identifiable information. Of the about 270 to 280 Systems of Records Notices at the Department, about 208, roughly, are Legacy Agency SORN's, meaning that they came over from the Legacy agencies that contributed pieces to make up what is now known as the Department of Homeland Security. So for Coast Guard, there might be Department of Transportation SORN'S. For Secret Service, Customs Service, or Federal Law Enforcement Training Center, those SORN's may be from the Treasury Department.

The 208 number has been fairly constant at the Department for the five-and-a-half years that we've been in existence. And early on when I became Privacy Officer two years ago -- doesn't seem like it, but it was two years ago -- I said that we were going to make progress and we were going to knock that number down fairly substantially. And the months rolled by and we never seemed to actually make progress doing that. And so I said, ''No, I really mean it this time, and we have some money that we can use to bring in some contractors to assist us.'' And we've made some great progress. We have gone through and looked at all 208 SORN's, which as you know, is a requirement under an OMB circular every two years to review SORN's to make sure that they're still viable, whether they're still needed, whether we should still be collecting that information. we've gone through and reviewed all 208 SORN's. We've looked to see where we can retire SORN's and go under Government-wide Systems of Records Notices. If that wasn't possible, we've looked to see where we could go under DH-wide Systems of Records Notices, either though existing DH-wide SORN's or by drafting new DHS-wide SORN's. And then for the remainder of the SORN's that were component-specific, we've gone about working on drafts of those component-specific SORN's to get back to the components so that they can review them, get them where they want them to be and we can get them published.

In addition, for some of the components -- Coast Guard being the most notable -- we went ahead and drafted new SORN's -- I think there's something like about 26 SORN's if I recall that are Coast Guard specific -- that we went ahead and drafted for Coast Guard and then sent over to Coast Guard. And we've done that for the other components, but Coast Guard was the first of the components that we did that for.

And we are on a rolling basis sending documents over to OMB -- Office of Management and Budget -- for their review, and then on to the Federal Register for publication. So, you heard it first before all of the trade publications write about it when they see all of these documents on a rolling basis being published in the Federal Register notice. That's why we're doing it; because it's good Government, because we need to have those SORN's updated, because it's an OMB requirement, because of transparency. So when you see them, there's -- there are no mysteries. We're just getting our documentation in order.

In a propos of a discussion that we had last night after dinner with the Chair -- and I understand at lunch we'll probably get into -- but, I understand that some of you may be unfamiliar with the federal process, and in particular, the things that happen every four years with respect to transition and priorities. And the Legacy SORN's are my number one priority in the next four months before the change of administrations. Getting that privacy documentation up to date and reflecting the way we do SORN's and not the way other agencies do SORN's is critical to the Privacy Office. It's our number one priority before I go out the door.

So on technology -- and I anticipate probably in December when we meet next, we'll be meeting in the DC area -- and let me pause. You may recall that last December we didn't hold a meeting, and that was because we were living from continuing resolution to continuing resolution. And I was concerned about it not being good stewardship of federal dollars to have an advisory committee meeting while we were waiting for our budget to be approved. There is the possibility that we may be living from continuing resolution to continuing resolution this year. I've talked to our Appropriations Counsel who are cautiously optimistic, and so we'll have to wait and see what happens over the next week-and-a- half before Congress recesses for the elections. I anticipate that we will have a budget, but we'll see. So, assuming that we do have a budget, I am anticipating that in December we will probably have a focus on cyber security and we'll have folks who are involved in the Administration's Comprehensive National Cyber Security Initiatives to come and talk to you.

Along those lines, I am sure you are aware that back in May we published the updated Einstein 2 Privacy Impact Assessment. Einstein is an intrusion detection system that -- actually, it's an improved intrusion detection system that is under US-CERT, which is a key player in the Comprehensive National Cyber Security Initiative. We published that document; it's one of the few public documents that's available on the CNCI, and if you haven't read it, I encourage you to do so.

Also, as part of the CIO Council's Privacy Committee, I was designated Subcommittee Chair for the Cyber Security Subcommittee. And so I and my staff have been working very closely with folks from OMB and the White House and ODNI and other agencies on the Comprehensive National Cyber Security Initiative.

And I'm pausing as I look over my notes because I did fly in last night so I could join you all for dinner, and so I'm a little behind the curve this morning.

A number of other things that we did on technology -- the Privacy Office is part of the Biometrics and Identity Management Task Force for the National Science and Technology Council; concluded work on a paper which will be released before the Biometrics Consortium Conference later on this month. The Privacy Office published a USCIS PIA update for the Person Centric Query Service [PCQS] and implementation of service-oriented architecture, and we work with USCIS to establish reusable template documents for further PCQ uses. And the Privacy Office is looking to the Data Integrity

and Information Protection Subcommittee of DPIAC to assist in developing a scalable, reusable privacy model for SON.

I note on testimony -- in June, I testified before Congress, the House Subcommittee on Information Policy Senses and National Archives Committee on Oversight and Government Reform -- the topic was agency use of commercial data-brokers and associated privacy issues.

Other panelists included our good friend Linda Koontz from GAO and also Karen Evans from OMB.

On the personnel front, and as a good bureaucrat, I would be neglect if I didn't talk about personnel. We made some significant progress in moving away from contractors and towards federal employees. And as I was reflecting last night on the flight out here about the changes when I came in two years ago, there were about 11 or 12 full-time equivalent federal employees in the office, and if I recall correctly, about 16 contractors. That number has changed significantly. We are somewhere around 23 to 25 federal employees and I think maybe five to seven -- five to eight contractors. The number of contractors are going to drop a little bit more, not appreciatably, at least during the time when we're working on the Legacy SORN project because those folks came in specifically to assist us on that. But when we're done with the Legacy SORN project, which I anticipate will carry into the next administration, those folks will go.

We added six or seven positions under the FY 08 budget. That was the first time that there was an increase of dollars beyond cost of living for the Privacy Office and the first time that there was an increase in federal employees, FTE's, for the Privacy Office. So fairly significant.

We have working with the General Counsel's Office hired one attorney and we're looking to hire another attorney. Additionally, we have hired an Associate Director for privacy policy and education, and we anticipate that person will be on the federal rolls at the end of the month; an Associate Director for Intelligence and Technology; a Senior Attorney from DOJ who has a substantial amount of experience within the intelligence community, and as soon as her clearances are passed and she goes through all the things that she has to do at DHS, she'll be on board and working very closely with the IC folks at the Department. And finally, we've got -- we've hired a director for Privacy Incidents and Inquiries -- someone we know from the DOD world who, once her clearance has been completed, will be coming over and joining us. And she has substantial experience in privacy over in DOD, which will give us, I think, some added depth of experience and coverage in the office.

And as I mentioned, we have finished the annual report. I am hoping this year that the only news on the annual report will be that the annual report is out. But having been in this job for two years and gotten at two of the three annual reports that the Privacy Office has issued, I'll believe it when I see it. Not that the report is getting out, I

am confident that it will, but that the media coverage won't just be limited to the actual annual report getting out.

On the international front, we've been doing a number of things. And I want to kind of go out of order here on the things that we've done because while it is not one of my priorities, it is I think a priority for the incoming Privacy Officer and the next administration. In May, at the invitation of Artemi Rallo and the Portuguese Data Protection Commissioner, I attended the Ibero-American Data Protection Network Conference in Cartagena de Indias in Colombia and had a wonderful time. I think it is important for the Privacy Office to become more engaged with Latin American privacy officials, just as we have done with European privacy officials. And I will tell you that I was disappointed in some of my American colleagues -- I don't think any of you were invited -- but some of our American colleagues who had been invited to attend and participate at the Ibero-American Data Protection Network, but were unable to do so. Privacy is of growing interest. Of course, if you're familiar with Latin American privacy, you're familiar with the -- I'm going to get it wrong -- Habeas Data, which I think is correct. I'm not a Latin guy. But Joe Alhadeff is shaking his head yes as is Lisa so I must have gotten it right. But privacy is of growing interest in Latin America, and doubtless will be an area where the Department not only has currently significant interests but will in the future have greater interest.

A couple of weeks ago -- maybe actually it was last week -- you know, at DHS if it wasn't today or yesterday it could be six months or two years ago and you're never really sure. Last week we had the second of our exchange programs take place. We had an official from the Spanish Data Protection Authority visit our office and work in our office from September 8th to September 12th as a way to gain greater insight into our respective privacy policies and programs. Our colleague from the Spanish DPA's office got a lot out of it and was -- I don't want to speak for her -- but we -- I gathered from my conversations with her, was very impressed with the way that we conduct Privacy Impact Assessments, which is something that they just don't do.

And let me jump ahead -- it's not on my notes but I wanted to mention to you that what I am anticipating in November of this year, two of our staff will be going to the UK to work in the UK Information Commissioner's office to have a better understanding of how the UK does privacy. And I think we are pretty close to finalizing that. I'm looking over at Becky [phonetic] and she confirms that. So as I said, sometime in November, a couple of our folks and someone from Compliance and someone from our International Privacy Policy teams will be going over to work in Richard Thomas' office for a week or two.

Next week Lauren Sadaat, of IPP, and I will be traveling to Brussels and The Hague. I'll be speaking at the European Networking Group's Executive Summit on Strategic Data Protection and Privacy. We'll be meeting with folks from the European Commission -- justice, law, and security -- as well as we'll be meeting with Peter Hustinx, the European Data Protection Supervisor. And then we'll be up to Brussels for

some -- I mean -- sorry -- up to The Hague for some meetings, and which after we finalize them, I'll tell you about.

The week after that, John will be traveling to Brussels to present at Nat Sec 08, which is a conference sponsored by World Wide Business Research.

And then in mid-October, as you know, is the International Privacy and Data Protection Commissioners Conference in Strasburg. I will be speaking on a panel titled ''Security Towards a Worldwide Identification Database;'' and no, I don't think we're moving towards a worldwide identification database. But if you're there in Strasburg, you'll hear the rest of my remarks.

Actually, as I saw that title -- and I don't know why it seems appropriate here in Las Vegas -- but as I saw that tile, I was reminded of that wonderful James Coburn movie The President's Analyst. And you'll recall the bad guy in that film was, of course, TPC - The Phone Company. So you may want to rent that wonderful film.

And with that, I'll stop. I have no further comments, either ad lib or off of my notes. So if there are any questions I'm happy to take them.

MR. BEALES: Thanks, Hugo. Are there questions? Lisa. And let me just say to the members of the Committee, these mics you have to hold the button while you talk. So this will keep short questions.

MR. TEUFEL: If you do it for half-an-hour, your hand is really tired.

MS. SOTTO: Hugo, thank you for giving us a terrific update. Just a quick question. Could you give us a little bit more detail about Einstein 2?

MR. TEUFEL: Sure. No, I say that because we did over the summer -- we did a number of classified and unclassified briefings up on the Hill, and I spent a lot of time talking about it. And so of course it's the one thing I didn't prepare for. It is similar to Einstein 1 -- and you'll recall Einstein 1 was one of the first PIA's that the Privacy Office issued, it's an intrusion detection system -- and Einstein 1 -- and I'm pausing here as I recall all of the details and the differences between Einstein 1 and Einstein 2. Einstein 1 looked at flow data. Einstein 2 -- and Einstein 1 was not mandated on all executive branch agencies. So not everybody was using Einstein 1, and it was only getting flow data, and it was after the fact. And so you might see some unusual amount of travel back and forth -- you wouldn't see it real time, you wouldn't know exactly what it was. Einstein 2 goes beyond that and beyond flow data to look at 14 signatures as well as other anomalous activity. And as part of the CNCI, Einstein 2 is being mandated on all executive branch agencies. Okay. That means it's not the judiciary, it's not the legislative branch, and I don't believe its independent agencies. I'm not confident on my answer there, but thought was given to what should be covered and what shouldn't be covered. So the things that are in the executive branch that report up to the President, those things are going to be covered. So it's going to be all the Cabinet-level agencies.

And as I said, it goes beyond flow data to be more comprehensive. And it will give the folks at US-CERT and others who are concerned about computer security within the government, a better idea of what's coming in, where it's going to, those sorts of things. And you can imagine the privacy issues were great with respect to Einstein and the CNCI as a whole. And without the benefit of being a little bit more prepared, I don't want to speak too in detail because I don't want to make misstatements that get it wrong. But a lot of thought was given to what is it that Einstein 2 looks at? And how will we make sure -- how will we make sure that Einstein 2 is not used to read people's emails and look at other things. And so the answer is, that's now what it's about. The Privacy Offices provided training will be involved in looking at the sorts of things that US-CERT will be looking at through Einstein 2.0. And it's not something that's interested in the content of emails, unless of course the emails happen to have viruses, Trojan horses, malware, bad things that we in the government don't want to have come in. Then of course the investigators will be brought in to look and see what's going on and why is this happening. But it's not a surveillance tool; it's a tool to make sure that the Federal Government has as much protection as the private sector does when it comes to the security of its computer networks.

UNKNOWN MALE: Just a quick question on the international. You know, one of the issues I understand, since the U.S. does not have a government-wide data protection commissioner or privacy officer, will your relationship with the international community, whether it's Latin American or but particularly European DPC's and Peter Hustinx; are you being -- you know, and the great work you guys are doing with international, are you being kind of treated as a primary U.S. data privacy representative to the European DPC's and their community? Could you just talk a little bit about your relationship with them and how that's working?

MR. TEUFEL: I think it would just be terribly bold of me to say yes to that, so I'm not going to. I know the last time Peter Hustinx came to our office and we talked about this subject, his question to me was, ''Whom do I go to see when I want to talk about the whole Government?'' And I'm -- I had hoped, frankly, that by now Dan Sutherland would have been confirmed to be the Chair of the newly independent Privacy and Civil Liberties Oversight Board, which I think may have some comparisons to Data Protection Commissioners over in Europe -- not quite the same but may have some comparisons. Unfortunately, Dan's not been confirmed. I was very, very hardened to see Jim Dempsey was nominated to be one of the members of the Board. But I fear that in the next week-and-a-half we're not going to see -- I mean, I don't know. But they may not be confirmed, and we are in Vegas so if I were a betting guy, which I'm not -- I would probably not put my money down on confirmation. Which is too bad. But a lot of the issues that are of interest to our international colleagues in the data protection community are taking place at the Department. And so even if there were a Privacy and Civil Liberties Oversight Board stood up, I think there would still be great interest from the Data Protection Commissioners as to what we're doing, and I think they'd want to come and talk to us. And an example of that would be the High Level Contact Group which is the joint US-EU ongoing discussions over shared principles or joint principles that we can then use for data exchanges in the future. And of course the Data Protection

Commissioners are not at the table for those discussions with the European Commission; I am, as one of the two principals from DHS to the HLCG. And so often folks from the Data Protection Commissioner's Office are interested to talk to us and talk to our colleagues over at the Policy Office at DHS about what's going on, and to the extent that we can talk, we do. But obviously we're not going to disclose ongoing negotiations that would hamper ongoing negotiations.

MR. BEALES: Thank you very much, Hugo. We appreciate your being here with us today. It's nice to have you back with us. I'm -- Ramon -- okay. If you have a quick one, we do have -- we do have a schedule.

UNKNOWN: [Speaking off microphone].

MR. TEUFEL: Cuba, Venezuela and Uruguay were not in attendance at the Ibero-American Data Protection Network Conference, unfortunately.

UNKOWN: I'll ask you my question offline.

MR. BEALES: We were -- according to our agenda, we were going to hear an update about fusion centers, but Commander Dan Wells could not be with us today so we're moving up the session that was scheduled for this afternoon on privacy technology.

And speaking to us today, we are very pleased to have Jeff Jonas, who is the IBM Distinguished Engineer and Chief Scientist at the Entity Analytic Solutions in the IBM Software Group. Jeff is responsible for shaping the overall technical strategy of next generation identity analytics. And use of that capability is part of the overall IBM technology strategy. One of his creations involves a technique enabling advanced data correlation while only using cryptographic hashes. This is a capability that makes it possible for organizations to discover records of common interests, like identities, without the transfer of any privacy invading content.

Jeff is a member of the Markle Foundation Task Force on National Security in the Information Age and he's an active contributor on privacy, technology and homeland security issues to leading think tanks, privacy advocacy groups, and policy research organizations including CDT, the Heritage Foundation, Center for Strategic and International Studies, and the Office of the Secretary of Defense Highlands Forum. Jeff, it's a pleasure to have you with us and we look forward to hearing from you.

MR. JONAS: Thank you. Is it true you have to hold the button?

UNKNOWN MALE: It appears to be the case.

MR. JONAS: -- for the hour? That's great. There might be a technological solution to this, but I have some friends around here that might help me with this. This is a great -- hmm.

UNKNOWN: [Speaking off microphone].

MR. JONAS: Oh, yeah. Is there any way the microphone could be -- is it -- will it reach? Is anybody in charge of that? Let's press on.

All right. Well, thank you for having me. I'd first like to say I'm speaking as an individual; everything I say doesn't necessarily represent that of my employer, IBM.

I thought I would today cover these four items and then do Q&A. I do a little background on my history and the way I see the world. Then a quick section on macro trends; what are the really big things that are happening?

UNKNOWN MALE: There you go.

MR. JONAS: That is real engineering.

So I'm going to cover some macro trends. And then I thought it would be fitting since we're in Vegas and I've built a lot of systems for the gaming industry, is just to take a look at what Vegas has done, how it finds a few bad guys, and how it does that in a way that gives consumers really a lot of freedom and a lot of anonymity. I was going to then close with some responsible innovation or in that direction, and this would be some conversation in the area of policy and technology, then Q&A.

So we'll just start with some background. I started a company in the early 1980's; I was building custom software. I built between 150 and 200 systems in my life for all different kinds of industries. Starting in the early '90's that became to -- or came to include the gaming industry. Built lots of different systems for gaming, ranging from tracking the fish in the large aquarium at the Mirage to the employment systems that were used for applicant processing with the opening of the Bellagio. But one of the more notable systems, and of possible more interest to the Committee, is the technology that became known as NORA, or Non-Obvious Relationship Awareness. And the goal of the casino is if you can lose $250,000 in 15 minutes to some scams, you don't want to wait till the end of the week to figure out that you've been had. That technology grew up, it was later -- took some additional funding from In-Q-Tel, which is the venture capital arm for the CIA. The funding in this in 2001 was prior to September 11th. The interest in our technology by the government was finding criminals in the organization. Then September 11th happened and we found ourselves in the middle of a variety of counter-terrorism programs.

IBM acquired my company in January of 2005. I'm the Chief Scientist of a unit; that's the remnants of my company, and I'm also an IBM Distinguished Engineer. The roles that I play today include -- I'm a member of the IBM Academy of Technology, I'm a member of the Markle Foundation's Task Force on National Security in the Information Age where we've been writing information-sharing policy reports. I'm also a Senior Associate for CSIS, and I'm doing some work on voter registration databases for the National Academy of Science.

My primary interests include making sense of lots of data in complex ecosystems with emphasis on privacy and civil liberties. Three example projects I've been involved in -- in '96 I built a system -- it was not for government, it was for an organization that had 4,200 physically different systems around the world. They wanted to comingle the data at what at the time, was estimated to be 80 million consumers and 1.6 billion transactions about them. It was for marketing purposes; they wanted to better understand who their customers were. Built that system, last I heard they had 5,000 systems feeding the central database on -- in excess of 100 million people.

In 2001, we did some work for the government and for the private sector related to post-9/11, 9/11 forensics. It was this work that led me to be very public about the fact that the shapes of networks actually don't help you find bad guys. If you think a shape of a network is interesting, you find soccer teams that are traveling, you find people traveling for family reunions, and the only time networks are valuable is when you have an entrance point and you know where to start. And so I published some work about how 9/11 could have been unraveled. That was later brought out in more light in the 9/11 Commission Report. But in essence, if you know a few bad guys and you chase a few threads narrowly, you -- 9/11 could have been averted and -- this is all quite public -- that you could have done it without new technology and even without additional law.

And then another example of kind of a complex information-sharing problem is, in 2005, with the Katrina hurricane, people were naming the missing and found in many websites. There were over 50 websites of the missing and found, and they were having difficulty reunifying people because they would mention that their father was missing in five websites but the father would be on the sixth website saying, ''I'm here. I'm here.'' We worked with the Governor's office and we took the 15 largest websites and 1.5 million people that had registered as lost or found, and we did a reunification project which led to the reunification of over 100 people. And you have to do a lot of policy thinking about this because you don't want somebody who is a debt collector or an estranged spouse to say, ''Oh, I'm looking for so-and-so,'' and then, thank you to the Governor's office, they'd become reunited. So a lot of policy protection mechanisms need to go into systems like that.

So that's kind of how I've grown up. Now a few macro trends, it's the way I see the world. And I think at the end of the day this is going to be relevant to how we drive on technology and policy and privacy.

I'll start with the good news: the world is not a more dangerous place. In the late 1800's in Western Europe the average life span was 37. Today, the global average including Africa is 67. You're going to live older today than any time in the history of mankind. Another example of this is in the 1300's, Black Death killed approximately 75 million people, that's about 17 percent of the world's population. And today if America sunk and we all bit it all at once, it's only 4.5 percent of the world's population.

So while that's true, I call this my more death cheaper and future graph. It's a tension point. The first nuclear device took 130,000 people and $37 billion, and in 1945

resulted in Hiroshima of approximately 140,000 deaths. The 1918 Spanish Influenza has been dug up out of the permafrost in an Eskimo and its DNA has been re-sequenced and published. It's been made public. I didn't believe this; I asked for a copy. If it makes you feel better, it's here on my laptop. And now that it's public. A team of less than 50 people spending less than $100,000 have brought it back to life in a laboratory, like a university lab, and put it in mice with the human immune system – it creates more death than any virus ever seen on the human immune system. And one estimate is that it would kill approximately 160 million people if released.

While that's the bad news, this is really about, in this day and age, more things can be done faster with fewer people. You know, in the -- 1870, it took Rockefeller many, many, many years to become a billionaire in today's dollars, and Mark Zuckerberg at Facebook has done this in less than three. That's good.

It's really all about competition, whether it's governments challenging governments or governments challenging asymmetric threats like terrorist, or companies competing with companies. When you're competing, you want to have the very best, smartest people; you want to have the best tools and you want to have data. And when you have tools, you want to be able to make the most sense of data, and when you have data you want the data first. There's a reason why the real estate closest to the Stock Exchanges in New York is reportedly some of the most expensive real estate in all of New York. It's because he who can get on the fiber first, sees it first, can trade first. And if you trade first, you are more competitive than your neighbor. Goldman Sachs was public about this; they said every millisecond gained in their trading programs is worth $100 million a year.

So at the same time, the damage potential per person is changing. This is kind of along the theme of more death cheaper in future; here you have a single individual, Jérôme Kerviel, this is at Société Générale Bank in France, creates approximately $7 billion in U.S. damage. This is a single individual acting alone or possibly with one accomplice, and because he knew the systems and worked for the company, there was a daily checkpoint. They had systems that at the end of every day would evaluate to see if there was any funny business going on. But knowing this, he backed in his transactions and out his transactions around each of these checkpoints in order to avoid discovery.

You take Muhammed and Malvo in the trunk of a car and, you know, you have two people with a hack that's maybe $3,000 including the car and the gun and the bullets, creates -- I think 12 people lost their lives and a half a billion dollars of economic damage.

And finally, in terms of a trend, as computers are getting faster, organizations are getting dumber. And this is occurring because the speed with which data is created and replicated -- copies of it is moving like this and the ability to make sense of it is moving like this. The gap is widening. If you can make sense of 8 percent of what you know today, in three or four years you'll know maybe 2 percent of what you know. You know being that the data or perceptions are observations that your organization has collected.

The reason why this curve is flattening out for sense-making is for the most part organizations have been staring at single transactions. This is kind of like just staring at a puzzle piece. If that's all you know is the single communication or the single report, it's kind of just like staring at a pixel or just a puzzle piece. And one could say that you could use an infinite amount of compute and an infinite amount of time and energy to try to study a single puzzle piece or a single pixel, as there is a real limit as to how smart you can be. And what's happening and where the future is going and where the tensions of privacy run head-to-head with this is, it's information in context that helps you understand each individual pixel or puzzle piece. If you can see that this email address is related to this other data and you can see that it's, you know, somebody that's subscribing to a newsletter, somebody's a term ''no re-hire,'' this means they've been employed but they've been terminated and they've been terminated in a way that they would choose not to hire them again, maybe they're somehow related to an existing customer, maybe a pending investigation. With this much context, information comingled, you could use a very minimal amount of computing power to make better sense of this.

And just looking to the future, this means -- or the way that organizations, business, and governments are going to get smarter is they're going to take individual transactions of data, individual piles of data -- the yellow pile of puzzle pieces and the blue pile of puzzle pieces -- and stitch these together. I think of these as like putting context to data, or call this context engines, and it's going to move this line up to make more sense of what you know. And so this is really a story about surveillance and surveillance societies. The ACLU came out with something called the Six Minutes to Midnight. It's their doomsday clock; it's how many minutes until it's a total surveillance society.

I got a call from some of my friends over there; they said, ''You should take a look at this.'' And I took a look at it and my first instinct was that maybe it's an overreaction. Could it really be six minutes? But after some thinking about this, I discovered six minutes is pretty plausible. I came up with a set of scenarios. I came to the conclusion that a surveillance society is not only inevitable and irreversible, but more interestingly it's irresistible. It's the consumers that are doing this, not governments. Everybody loves GPS. You can find Starbucks; you know where your kids are. My friend was saying, ''Look, I got a buddy, he's driving somewhere now.
Look at my phone, I can tell you where he is. If he tells me he's five minutes from the house, I can tell he's ten.'' And, you know what? He loved it. RFID everywhere; RFID in your glasses? Yeah, you'll want that. You won't lose them again. This is the trend.

And this is going to lead to -- if you think there's a lot of sensors now, there's going to be even more sensors. Sensors are going to become more ubiquitous. And the piles of data that are now discreet are really going to become one and it's going to become one because organizations want to service the consumer and the consumers are going to gobble this up as we optimize our lives.

So information and context is going to be data from many sensors comingled to make better sense of it. And it's going to live up in network clouds. You can think of

this as collective intelligence. And as data is changing in the universe, it's going to be stitched together in these large databases. And I give you a little prediction now about 2050 -- collective intelligence will locate what you need to know and tell you. It's not going to be like Tom Cruise in Minority Report with the gloves and he's moving images around and looking for stuff. The future is going to be this data being stitched together and delivered to you, and then you're going to eat it up.

And on somewhat of a humorous note, the way this might work is that in the clouds there's a bunch of data about you where you are right now on earth, physically -- latitude, longitude, where you are geospatially. And there's, let's say, another bunch of data completely unrelated to you about the behavior of migratory birds. Yet there's a sensor and the sensor is near you and it's doing wind speed. And when this sensor produces this piece of data, it recognizes that there's a relationship between some migratory birds that are being observed and where you're standing. And that cloud tells you to jump to the right one foot, so you jump. And here comes a bird dung, and it just misses you. And so this is really the future, is that when it serves you and your doctor you're going to love it, and when it serves the police looking at you, you're going to hate it.

So, I thought then I would just, again -- it would be fitting since we're sitting in Las Vegas, where there are possibly more sensors per square inch than almost anywhere on earth, maybe except, a space shuttle or a battleship. So let's -- I just would like to take you through this as -- yeah, anyway. Hold on.

Do we have any questions so far, any burning questions that you can't think anymore because it's such a big question? From the committee? No, fine.

Okay. So just a little bit about Vegas. It's one of the fastest growing cities in the United States; 38 million people come here a year. Australia receives 20 million visitors a year, Vegas 38 million. Eighteen of the 20th largest hotels are here. A mega resort will see over 100,000 people a day in a single location. Each casino contains tens of thousands of sensors and over a hundred information systems that collect, analyze, do discovery, stitch the data together, and make sense of it.

There are some fundamental gaming principles. The idea is to make it fun and well worth the price. Mirage Hotel was the first to have the majority of its revenue not coming from gaming; it comes from other things -- shows, dinners, retail, and the hotel. Problem gamblers are bad for business. It doesn't make the industry look good; they would prefer to keep them out.

The business is optimized for the consumer experience over interfering with the consumer. The surveillance and security, while it does protect assets and you're looking for cheaters and people who are card counting, it's just as much trying to protect the consumer from somebody walking along to steal your purse, take the money out of your machine kind of behind your back if you're not looking, and manage the integrity of the game. They want to make sure that everybody at the game has an equal shot at the game.

One of the problems they have today is sometimes in poker you'll have three or four people that are really part of a team but nobody knows. They're signaling each other; it's really unfair for the other players to not know that.

When it comes to spending money, there's this idea that the surveillance and security must be -- get massive amounts of funding. In truth, they'd rather make the carpet look better, put another slot machine in. They spend a minimum amount of money on security and surveillance. And when security taps on somebody's shoulder and actually removes them, it's really for egregious behavior. I've been in the surveillance room, watched them catch somebody cheating; they'll send security to go talk to them and say, ''We saw you cheat. Don't do that.'' That's it. They left them with a smile. So they favor the false negative. They'd rather not kick somebody out and get that wrong. It just creates a bad image.

It's a loud feedback loop in gaming. If you kick somebody out that's good – or inappropriately -- it's a very loud event, and if you miss something that you should have caught and it was a big loss, it's a good feedback loop.

There's this notion, ''What happens in Vegas stays in Vegas.'' I joke about this. I say, ''And it also stays on video.'' I joke about that and say, ''But the good news is they throw it away every couple weeks.''

But they really -- they worry about unintended disclosure of personal data. It's happened in a very few cases -- I'll touch upon that in a minute. And there was some news about National Security Letters used for the collection of information from gaming, and one casino I think was on record that they just said, ''No.''

So the question is, from a casino's point-of-view, ''Who are you?'' You can walk through a casino with cash; if you don't go to the cash machine and if you don't use your credit cards, you can show up, you can walk into the casino, you can gamble, have dinner, see a show, and never introduce who you are. Now there's a point where you reach a financial transaction threshold that you have a -- casinos have an obligation to -- in support of IRS regulation, the prevention of money laundering and the U.S. Patriot Act where they have to start finding out who you are, but for the most part you do not have to describe who you are. It's a great privacy point for anonymity.

But they might ask you, ''Do you want to join the Players Club?'' I mean, if you're spending a lot of money, that's -- would be a way they would come to know you because they want to give you a room and a meal if, and compensate you appropriately. There's some points where they need your ID; they want to make sure you're over 21. There's the IRS thresholds for taxes and CTR thresholds -- Currency Transaction Reports. They have an obligation -- this -- if you show up and are playing in one pit area and then you switch tables and then you switch pits, then you go to your room and change, take a shower and come back and play in another pit, they have an obligation to know if you have won more than a certain amount of money over a 24-hour period and they have an obligation to report that even if you have not identified yourself. They

haven't chosen to RFID tag everybody; it's their obligation to try to figure that out, and that's their ability and it's done with humans to share this information and do their best to see what the total transaction win amount of somebody is, if it crosses a threshold. Disguises are welcome. You want to dress up like Elvis, no problem. But false identity documents are not.

But are you a subject of interest? Well, there's the U.S. Department of Treasury's OFAC -- Office of Foreign Asset Control -- Specially Designated Nationals list. It has money launderers, drug cartel folks, and notably it's grown recently with names of terrorists. They are obligated not to do business with them. There are people that they've already 86'ed -- it's a law enforcement term of kicking people out of their -- or off their premises -- and trespass them; it says you can't come back.

People who have already been accused as gaming felons are people that they would like to know. People who are known cheaters -- they' haven't been arrested yet but the industry shares some information. And then there's advantage players; now, this is card counting -- the softer, gentler term is advantage players. And these are people that can use their mind to change the odds of the game. Most people who card count make a few mistakes an hour; even one mistake an hour you'll still lose money. But the casinos feel that if you can use your mind and change the odds of the game so much that you've turned the casino into a bank, they can ask you to play a different game.

There's a self-exclusionary list. This is where people say, ''I'm a problem gambler, I want to self-select myself, my name to that list and please don't market to me.'' In fact, if the casinos keep luring them in -- there have been some suits about this -- somebody puts themselves on the exclusionary list and the casino then sends them a promotional material and it says, ''If you come on Friday, we're going to put you in the slot tournament for free and we're going to give you a room'' and they did this and lost more of their assets or lost their house or whatever, and then they said, ''That was just mean 'cause you knew 'cause I told you.''

And then the Gaming Control Board has an exclusionary list. It used to be called the Black Book or the Black List, now it's called the exclusionary list. This is the equivalent of an OFAC list for gaming if -- it's run by the gaming regulators, it's public, you can see it on the website, if you're on it. There has been due process, there is an appeals mechanism. And from that website -- I just took this record off. No reason I picked this one over the other 30 or 40 names that are on there -- but this person has been, doing stuff to the gaming industry for some time. And that's the way that would look.

So, Vegas is an interesting target for opportunists because there is a lot of cash that changes hands. You know, a lot of cash changes hands in a bank, too, but at a bank the outcome of every transaction is certain. In gaming, because the outcome of the transactions aren't certain, the patron can sit there with $80,000 in chips and say, ''Hey, look, I guess I got lucky.'' So that opens the door for the opportunist. And it's easy to think that one can get lost in the heavy volumes. You'll find more people trying to

perpetrate various attacks on casinos during fight night and big weekend events just because there's more noise.

There are all kinds of scams for beating casinos, including illegal devices. I mentioned advantage players, recruiting one's own employees, there's money laundering risks and credit and check fraud, there's slip-and-falls, insurance scams. We've had armed cage takeovers where they jump into your cage with guns and steal your money, and we've had an executive's daughter kidnapped -- rescued safely from the trunk of her car. So we see all kinds of attacks on the industry. And they try to mask the bad actors; they use false identities. They have -- one guy I know of has 32 AKA's, he uses four or five Social Security Numbers, four or five dates of birth. They recruit people far away you've never seen. They've trained them in rogue labs. They bring them to the casino; the first day they step foot in the casino they're an absolute professional at what they're about to do. And they might take your high roller, somebody you've trusted for years, and they might recruit them in the bar and say, ''You want to get on the plus side of this equation? We're going to make you part of a scam. We're not even going to tell you what it is -- how we're going to help you win, but you're going to win and we want a cut of that.'' So you've gone from somebody you've trusted for years and years and years, and now they're winning -- which would be normal; you can have up -- you have wins and losses -- and it would take some time before they would detect that the wins now are really inconsistent with the losses.

There are different kinds of sophisticated attacks. There's coordinated card count teams where they've got two or more people at a table that are all working together secretly. People have been working for the manufacturers of the slot machines and imbedded code inside the chips -- the personality chips -- that cause the machines to pay a royal flush if you use the bet buttons in a certain series. So that was an insider job.

Somebody watched the roulette wheel of a casino for weeks and modeled every single drop of the ball. Used computers and figured out that the wheel had a bias; it was not perfectly balanced. And if you played to the bias, which they did, they won, I think, $5 million over two weeks. A key point about this is what is a remedy for this? Do they inspect the consumer more, do they make it -- do they raise the barrier on everybody that comes? No. They have a new policy and practice about how they ensure that the roulette wheels are balanced.

Somebody else used -- there' something called shuffle tracking. If you have a lot of tens -- if there's an area of the deck -- card counting and shuffle tracking is the idea that if you know where there's going to be a lot of tens in the deck, there's a reason why it benefits the player. Well, card counters are just trying to figure out if there's a lot of tens left in the deck. But shuffle trackers figured out that if you track where the tens are in the deck now – it is possible to determine where there there will be a lot of tens after the shuffle – thanks to the use big computers they use to figure this out. They've modeled the shuffle.

People are marking cards and -- not in the U.S. but in a foreign country one scam artist used radioactive material on the cards to mark them and then a Geiger counter to see it. Others will mark the cards with a material -- they'll put the dobbing material near their ear or in the pocket of their hand here; they'll mark cards with a material that the naked eye can't see but only with their contact lens can they. Marked cards would be bad; some people try to mark them at the game by bending them. Somebody else got up into the manufacturing model and modified the die. They were printing marked cards.

And we had a security consultant who used to be a cheater, then they came along and said, ''Now I'm a good guy. I'm going to help you all protect yourself.'' And then he later returned to being a bad guy and he built -- when you watch the World Series of Poker on TV, they've got the camera underneath so you can see all the cards? Well, they created a table like that and they went to a casino in Atlantic City and were recruiting people that had been -- eliminated in a big poker tournament, saying, ''Well, do you want to still play? We've got a private game upstairs.'' And the security consultant himself was the one orchestrating this.

And despite all these attacks and despite all the policies and procedures that one implements to protect oneself, you end up with scenarios like this. An organization – a casino -- it's called Regulation 6A by the gaming regulators -- but it's an obligation of casinos to record transactions over a certain amount, and it's also the same kind of threshold that's used for the Currency Transaction Reports which go to FinCEN. Well, a casino can be fined heavily for each one they don't file. But this particular individual over an 89 week period -- while the systems were correctly producing the reports -- this person decided to never mail them in. They discovered 15,000 of these -- I think the potential fine was in the hundreds of millions of dollars. Now, they discovered it first, the casino, and self-reported. Had this been discovered by somebody else, by the regulators, for example, ''How come this casino is no longer sending them?'' That would seem like a normal tripwire somewhere, but I digress. But it turned into a $5 million fine. A commentary on this from the University of Las Vegas said, ''but if you're paying somebody $10 an hour that leads to a $5 million fine, and the individual said, ''I didn't even know they were that important.'' Well, you would call that an administrative screw up.''

So about casinos and tripwires, if you were to go to a surveillance room, a casino may have 2,000 cameras but it'll have 50 monitors. While all the cameras are being recorded -- the gaming regulators require that the video is kept -- generally it's on tapes still these days, but the newer casinos are going digital -- but it's kept at least for a week by regulation. Some casinos keep it that long and some casinos keep it a little bit longer, but it gets thrown away unless there's evidence of a crime and they'll keep just that piece. But you're sitting there in the surveillance room and the question is, what do you look at where and when? I mean, you only have a few surveillance operators looking at 50 monitors connected to 2,000 cameras. So this is really about information triage.

So one of the things that they'll do, is they have watch lists, they know people that

have been 86'ed, they know people who are on the OFAC, and they know people who are on the Gaming Regulator's exclusionary list. They have an obligation to make sure these people do not check into their hotel, getting credit, being comped. They have Hot Player in the House; if somebody shows up, it's information triage -- not for a bad guy but if you have somebody that's really known as a great player and suddenly they're there, they want to know. But as much as anything, they have human eyeballs. It's the dealer's job to watch the player. It's the person -- the floor supervisor's job to watch the player and the dealer. It's the casino manager's job to watch all the floor supervisors and the dealers and the players, and it's really a whole stack of people watching other people create a whole series of protection. And when somebody sees something out of place -- sometimes it's a player -- one player actually watched another player take a stick -- watched the dealer, excuse me -- watched the dealer stealing chips off the table by using some sticky stuff . They had sticky stuff on their hand and it would move the chip off the table and then they would drop the chip into their other hand. And they reported this. By the way, this turned into one of the procedures now where the dealers clear their hands. When they're done, you wonder maybe why they put their hands up. Well, it shows the player and the cameras in the house they're not walking away with chips. So, again, many of the times that there is an attack, they just look at what policies and procedures can you put in place that don't sit on the consumer but sit on the house.

The door key systems -- if somebody loses a door key and now they're using the electronic keys in different doors -- some of the systems do this -- if you find a key and you're just sampling it door-to-door it actually triggers an alarm. Now, if you have volcanoes or big water cannons that can hurt people, and on New Year's Eve people are drinking and think it's fun to swim with the fire, it would have a laser -- there's a laser perimeter detecting people -- that flags an alarm and shuts off the fire. And there's machine-generated alarms; you open a door of a slot machine, there's a jackpot -- these things will draw attention to the machine so you can apply surveillance, a finite set of resources looking at the things of most interest.

As well, there's environmental and life safety sensors. And then there's back of house special access areas, like the computer rooms and where they count the money where there are more sensors than other places.

And just a few other things about gaming. I mentioned earlier there have been some unintended disclosures. There has been -- somebody did leak a widely known public figure -- I forget -- they were a government executive -- the fact that they were playing was leaked. This is a rare event. I remember another time one of my gaming customers discovered that there were boxes of paper with reports of player transactional data that had blown out across the street. I was out there helping fetch it.

Every game has a known winning and losing percent. I mean, how much you're going to win over what period of time. And if somebody comes in and plays a strategy on blackjack that you have never seen you might want to know what it's going to cost you or what it's going to be worth to you. So I have known of a case where a surveillance -- somebody is playing, they're playing with big dollars, so they would just

say, ‘‘Well, the strategy they’re playing with is like this.’’ And the computer plays that a million times and says, ‘‘This is how much this game is going to cost you, or cost them over time.’’

Some organizations spend a lot of money integrating the data and making better sense of it. Harrah’s has spent over $100 million to better understand their customers.

And casinos do exhaustive background checks on people who are handling the money and the executives. And it would rival any federal background check up to but not including the polygraph. And because you don’t want your surveillance people comingling with your dealers, some casinos want the surveillance people to not dine with the dealers in the back of the house dining rooms. And they might put them in a separate payroll system with the executives so that it’s not generally known who the surveillance people are. You want to separate those.

There’s information-wide information sharing. There is an organization called Griffin Investigations, and their job is to take data that is happening across the casino industry, and the casinos can self-select when they’ve been -- when they’ve had -- whether it’s card counters or cheaters attack that casino, the Griffin organization receives this from member casinos. And if they see somebody that’s showing up enough on a wide enough basis, they will republish it and make it available to the other member casinos.

And in interest of time, I’m going to get us back on track here. I’m jumping to chart 49. So what about privacy and anonymity? I mentioned people are free to come and use only cash, video is thrown away. There are no metal detectors like Macau. There are no identity check points where you have to come and prove who you are to get in. The casinos exercise great caution when they go to communicate with a player about their behavior. The surveillance department doesn’t actually do anything other than produce intelligence, some information, and an assessment. And then it’s the people who have the context on the ground who help decide what to do about it. They err on the side of friendly. When the casinos do share information, they share on a narrow basis.

Internet and public records are not collected on the patrons. There is no predictive data mining to spot the unwanted behavior. Most of the vulnerabilities are remedied with process not additional electronic surveillance. Most signals detected by humans; anytime something is detected by a system, it’s not put in the trigger, it’s actually given to humans to do something about. And their systems favor the false negatives.

Just to cover a few points on fact or fiction. Have casinos specifically targeted ex-felons to hire them on purpose? Answer is yes. Just in terms of community outreach, they found, -- and reduced recidivism, they wanted to see if they could find people in felony community that they could trust enough in certain jobs.

Do casinos perform background checks of guests on public records? No.

Is facial recognition used? I deployed facial recognition for the casinos in '96, by the way. But is it used to monitor everybody that's walking in the casinos? Absolutely not! It doesn't even work that well. They couldn't do it if they tried.

Is there a watch list you can put yourself on but can't take yourself off? Yes. If you say you are a problem gambler and now it's Friday night and you're drinking and you say, ''Can you take me off so I can get in?'' The answer is no.

Does the gaming industry offer assistance in the creation of false identities? Absolutely. In fact, the convention center has an invent-your-own-identity website. You can go there and it'll help you pick an identity and a name; it'll print business cards, it'll give you an 800 number. It's a fairly weak cover, but there is a cover.

And so, now, finally, I would want to talk more generally about responsible innovation. Some of these things learned from the gaming industry, some of these things learned by my ongoing conversations with organizations like ACLU, EPIC, EFF, Center for Democracy & Technology, and others. It's really important to engage the privacy community. I think there's not enough technologists and not enough policy people actually in conversations with people in the privacy community, and I think there should be more of that. I think one of the better examples of this is Tim Edgar's move from the ACLU to the ODNI's privacy group. Around the same time, somebody from the FBI actually moved to ACLU. I think that's good. I have more information about this on this link. I'll provide these references following this testimony for your website.

Insist on information attribution. You know, there was a time -- I have seen a watch list somewhere in some organization, and on the watch list there were some records where they didn't know who told them or why they had it. That would be a problem. You wouldn't know how to delete it if it was no longer accurate and you wouldn't know who to ask if something ever actually matched. So when you do hold information, it's absolutely paramount that you know who you got it from and who you could ask about it.

Data destruction. There's a point where you don't need the information anymore; it might be by law or it might just be good practice. I did some work -- I did a blog post on this called ''Decommissioning Data.'' I did this project -- one of the things that I have learned, this came from a conversation I had with David Sobel at the time at EPIC, now at EFF, and he was talking to me and I was being a student of privacy and I realized that I'd built this one system and we built it to solve a certain problem but after the problem was done, the data lived on. And I -- that caused me some tension as an innovator. So a future program came up where they're working on a certain problem, and I mandated in working this problem that when the problem was over -- in the contract -- the data would be discarded because it was done. And I was quite proud of myself for a few years after this, because I had learned something and it implemented an improved way. But later I had realized that after the data was destroyed there was no ability to be accountable for why the system behaved like it did. If the system actually missed something bad and

somebody was damaged, then they'd come to me and say, ''Mr. Jonas, how did your system miss this match or match this when it shouldn't have? Please explain.'' And I'd have to say, ''The evidence is gone, I've destroyed it.'' So this led to some thinking that I've had in this area -- over time you could make the data less and less accessible. So over time it's not as accessible for data mining, but maybe accessible for forensic purposes, like, maybe at the end of the day it's just printed. But then you could scan it, so maybe it's printed with the funny little letters where it's half marked through where only a human eyeball can read it. Except they're hacking through that these days, too.

Limit data transfers. I spent a lot time on information sharing, and I call it the information sharing paradox. If you can't share everything with everybody -- which is really impractical -- and everybody can't ask everybody every question, then how can anybody ever find anything? And it turns out the only way to really make information sharing work is to have a form of an index -- to solve discovery. It's who to ask for what. And the only way discovery works on earth today that I've seen, is directories. You search Google, it doesn't roam earth for it, it goes to the Google index. If you go to the library do you roam the halls? Nope, you go to the index. There's example after example.

And when the government thinks about information sharing, a way to limit information transfer is just to have an index, much like a library. And the library cards point to who's the holder. Now you have to ask the holder for it, so there's some transparency into what records you can see. And there's policy about whether you can see it or not. I've blogged extensively about this.

Another key thing one can do with technology is data tethering. If an organization creates data and transfers it, they need to know who they gave it to that way if it changed, you can say to the people who have received it that it's changed -- it's been redacted or, ''Sorry, we had the wrong passport number and it's really this number.'' This is very key. And it gets very hard to do because sometimes there's more information transfers than you think.

After being asked by friends in the privacy community over and over, ''Now, since you've built a lot of systems over your life, how many copies of the data are there?'' So I decided to blog post on this and the answer is, it's roughly equal to the number of licks to the center of the tootsie pop. If you remember this commercial, it's lick, lick, lick -- and you get kind of frustrated because you're not sure, -- it's going to take a zillion. There are cases where -- in almost every case there's over a hundred copies of a piece of data, and it's primarily due to backups. But data goes to primary systems and operational data stores and data marts and it goes to reporting systems, and then each of those is backed up. And then it goes to other partners and other operational systems and they put it in their data warehouses. And there are cases I know of where a single piece of data ends up in 10,000; 100,000; and possibly even 1,000,000 places. Data tethering can be difficult when you're talking about that kind of replication. But nonetheless, I think it's important.

I also think it's important that when you are going to have data, you need to try to obfuscate it. There's -- if you don't need the data with personally identifiable information for your analysis, you should obscure the PII.

There are also techniques for anonymization, some that I've worked on or invented myself, that allow you to anonymize data on the edges and do deep, analytic correlations on it while it is anonymized. And while none of these systems have any form of perfect protection, they do reduce the risk of unintended disclosure.

For systems that are -- especially systems that are non-transparent, especially for government systems, there's this notion of immutable audit logs. I wrote about this in a standalone paper for the Markle Foundation around national security; I penned this with Peter Swire. It's also been picked up in some work that's going on in healthcare. But it's the idea that you want to see how somebody's used a system. Have they used it within policy and law? And you want to do it in such a way that it's indelible, it's tamper resistant. It's that even if the DBA wanted to conspire and hide the evidence of how people have used the system, they couldn't; it's really etched in stone. And that's the notion of these immutable audit logs.

A few thoughts on data mining. Data mining in itself isn't bad. It's used, it helps -- it's probably the reason more people wear seat belts; many lives are saved. It's most useful when there's lots of evidence of good and bad or people hurt and people not hurt.

In counter-terrorism, predictive data mining, where there's a limited number of training events, historical terrorism events, this actually doesn't have that much efficacy. Jim Harper, on your committee -- and I actually co-published a CATO paper on this, I'll submit that as reference. And a place where I think data mining does work is predicate triage. Now, maybe predicate is the wrong word but I've come to kind of like it so I keep using it. But it's really the triage if you already have a list of known bad guys. If you have a list, and our government does, of people who are in the United States on expired and illegal visas -- and there's too many people on the list to go after all at once -- you could us data mining on them because you -- they will already meet a certain threshold. And you would use the data mining to glean the top ten you should work on first.

I've done a lot of work on link analysis. It's very powerful, especially -- and mainly when it's used in a narrow fashion. It works well when you have a subject of interest and you're looking out. Just link analysis across all of the good to find somebody who's bad, I don't think has that much efficacy. So I've done some publishing in the area of predicate-based link analysis. And a key thing on this is prune early. When the bad guy is connected to his mother, and after a little bit of inspection you realize mother is not involved, then there is no point in linking mother to somebody else, you prune.

Watch lists and false positives. I worked on a paper with Paul Rosenzweig while he was at Heritage, on the way to help address the matches -- the false positive hits on the TSA selectee and no-fly list. I get calls all the time from friends who say, ''I can't believe they have my name on the list.'' I'm, like, ''Your name's not on the list.''

There's a distinction between being wrongly named on the list and being wrongly matched. And the problem with many watch lists is they're low fidelity. And when you have a low fidelity watch list, it really is the driving cause of these false positives. It's just pathetic, quite frankly, because then everyone has heard just add or change a middle initial. ''Oh, don't use the middle initial "W", use William,'' and you're free and clear.

So, here's some related papers. I'll not cover these here. The one I will mention is that Stewart Baker, now Head of Policy at DHS, while at Steptoe & Johnson wrote a case study related to my anonymization technique, in relation to the EU Data Protection Directive, and the transfer of PNR data, EU to the US.

So in closing, final chart then questions. Here is really the future. There are going to be more sensors and more data. The data is going to be comingled more and more, primarily to serve the consumer, but the government will have to do this as well.

What data is collected and observed is really the debate. How smart do you want the government to be? Do you want it to be able to see the phone book? Huh? Yeah, it's a form of widely available data. Is it okay to see the phone book? If they can see the phone book, is it only on their desk or can they load the phone book? Huh? It's on the edge of the open source debate.

The chief privacy principle is avoid consumer surprise. If I were to summarize everything I've learned from my time with the privacy community, is, if you can avoid things that would surprise the consumer later, then you're probably better off. But if it's been collected and now an organization has a copy of it, they're actually, in my opinion, obligated to make sense of it. If you have the data in one pile and you have data in another pile and you haven't actually stitched it together and you actually miss some big crime -- and then in after-the-fact forensics you study it and you realize, ''I had some data in my pile and one door down in the agency they had a piece -- they had the relating piece of data in their pile,'' I call this enterprise amnesia. Huh? It's when one hand doesn't know what the other hand has. So you have obligations to make sense of what you know.

But a tension of this is that professionally bad actors really know how to hide themselves. And if you want to catch them in data, then you have to try to find observations -- this is how you catch a liar -- you have to find observations they didn't know you had. And this is where the tension is. How do you avoid consumer surprise and make sure everyone knows what everybody's collecting, and then at the same time, find a bad guy where you want to collect something that he didn't know you knew?

I have just one quick story on how to catch a bad guy. If somebody's lying to you how will you ever know? Your neighbor is a bad guy; how would you know? He's been telling you over and over, year over year that he's never traveled outside the United States but it's a lie. But then one day you go to a barbecue, it's his son's birthday and his wife's had two beers. And his wife says, ''You know what? Ever since he lived in

France, my husband's hated the French.'' Well, there you go. You've got the liar. And you've done that because you've increased your observation space. So that's the tension.

I blog here. And I hopefully have left a few minutes for questions.

MR BEALES: Thank you very much. It's been a fascinating presentation. And if you would provide us with a copy of the slides, that would be greatly appreciated. We would all be interested.

We are videographing instead of transcribing today, so we're going to pause for just a moment so the tape can be changed so that you can leave Vegas with us.

MR JONAS: I would like the chance to review the transcript to make sure it's been correct, you know, it's accurate.

MR BEALES: Sure. We can -- I think we can -- [End Tape 1, Begin Tape 2]

MR. JONAS: Okay.

MR. BEALES: All right. Thank you. David Hoffman.

MR. HOFFMAN: Jeff, thank you very much for your comments. I wanted to probe a little bit on one of your last comments and your conclusion about an obligation to analyze the data that you have. And I just want to expand on this with a comment and then get your reaction. I wonder, though, how much there is an obligation to analyze the data that you could get, which is, I think, different from what you said. Remarkably different. And -- because I'm struck by -- during your presentation the extent to which we could see a casino as a small country, a small society, and almost think and relate that to the efforts that we take as a country. What seems to me to be -- the one thing that's very, very different in the casino context is that people always have the ready ability to say, ''I do not like the experience of this casino so I'm going to choose to go play in the other casino.'' And I think most folks in the United States would say as patriotic Americans we wouldn't want to have that kind of market relationship where we would just say, ''I don't like it today here, I think I'm going to go play in some other country,'' which creates a market dynamic of saying for the casinos of -- from what you laid out here -- that the casinos really bend over backwards to not analyze all of the data that they could get given all of the sensors that they have and given how you describe the control rooms as being huge numbers of cameras and sensors and actually very few monitors, and that most was relying upon the abilities of the individuals acting in control roles. So I'm wondering if you could relate that and say, is there an analogy there that we could reach for DHS and for the country about this question of obligation to analyze all the data you can get versus all of the -- an obligation to analyze the data you retain.

MR. JONAS: All right. So, yeah, there's a few things on this. The thing about making sense of what you know is -- I don't think on one hand we can tell organizations not to make sense of what they've collected, but then on the other hand blame them for

missing the obvious when after something bad happens, it's self-evident that they knew. Huh? If you can't -- we, I think, as citizens shouldn't try to play both cards; that's not fair.

There's also the problem of instrumenting for the lone gunman. It's just too expensive; there's just -- you just need too many sensors, and you have to just let some things happen. Casinos are willing to absorb some risk. They're going to let some bad things happen. Muhammed and Malvo were in the trunk; what would it take to make sure that lone gunmen couldn't ever do that again? The kind of instrumentation you have to have on a society is too great. There's a point in technology where you say, ''We're not going to use technology; we're going to let bad things happen.'' Unless -- hey, let's put a satellite, you know, an antenna on everybody's head; we can save a thousand lives a year. Who wants to sign up? Most would opt out.

So the question is, do you really have to know everything or don't you? And I'm arguing that you don't always have to know everything. Resilience is going to cover you for part of that. Now, nuclear weapons make that scary. There's a risk threshold if you think something's going to happen in a big city, in the next week, one would raise the bar about what is fair to collect.

But you're right; there's no opt-out as little governments -- each casino is a little country in itself. Consumers can opt out and go from one to another, but casinos are so focused on not creating that experience. They're hyper-focused on that. They want to make it where you'd rather come to their casino than any other. So they favor in that direction.

Did I answer your question?

MR. HOFFMAN: I think you did.

MR. JONAS: Lucky me. Okay.

UNKNOWN: Ramon.

MR. BARQUIN: Jeff, I just want to go back to this issue of, you know, simplifying measuring risk by the probability of an event happening and the damage, if you will, the consequence. And this is where, to a large degree, I think that we have this difference between what the government believes it has to do in keeping the homeland safe, versus what -- not just a casino, but any individual business -- has to do to try to assure that it's minimizing risk at its own level.

And what guidance, I mean, again, coming back to what can we learn for homeland security vis a vis what the casinos have done? What kind of guidance can you provide here?

MR. JONAS: I think that the casinos -- and I think the government should as well -- the casinos optimize for business. They optimize to make it more efficient for consumers, they optimize to make it easier to come and play and transact. They don't really create a lot of sensors. They add sensors because they have a compliance obligation, like surveillance cameras, or because they want to better service the customer.

So I'll just give you, like, an example. And I haven't spent a lot of time on the whole RFID and the passport subject, so if I miss some fundamental elements, fine. But, if I was thinking RFID and passports, it wouldn't be to protect a society, it would be how can we make it more efficient for people to travel in and outside the United States. I'd optimize around that. If there was an ancillary benefit around how to make the country safer, like fake credentials, well, so be it. You're not creating the sensors just to chase bad guys; that's kind of an endless chain of cat and mouse. Huh? So I lean more towards add sensors if you're trying to help people optimize, and where possible, give people the right to opt in and out.

In truth, the casinos -- about risk management, there is not a lot of risk at the casinos. Every single game has a known hold percentage. There's -- when there has been risk, they look at what new policies and procedures they can implement that are going to sit on the side of the house and not affect the player. Yeah, a few exceptions -- they've figured out that people were putting cameras on the games. And so they said, ''Look, we don't want you sitting on the table using your cell phone.'' But anyway, much of it is policy and procedure.

MR. BARQUIN: If I can just follow up on that. Because you said, ''If all of the sudden there is a nuclear threat, you have to raise the bar.'' And what I'm trying to sort of get here, you know, if possible, is what exactly does that mean in terms of activities --

MR. JONAS: I see.

MR. BARQUIN: -- around the area of whatever -- data mining, link analysis, predictive --

MR. JONAS: Yeah.

MR. BARQUIN: -- modeling, that could help to do this while minimizing, you know, violations or civil liberty, privacy, et cetera?

MR. JONAS: Well, one -- there's like three questions packed into there. But, if you need to comingle data, like, one of -- right now, Section 215 of the U.S. Patriot Act makes it possible for the government not to collect a few records about a few people. But, say there might be records about a few people in the data set; we want a copy of the whole data set. That's a pretty big shift from the old day where you'd be, like, ''We need a record about Billy the Kid. Do you have anything on Billy the Kid?'' Now, I understand why someone -- a government might want to do that. The list is secret, and you can't give the secret list to the cruise line and you can't -- you don't want to read the

whole list to the cruise line. One remedy for that, which I get excited about, is the use of anonymization, where both sides could anonymize their data and you can find out what three records you want to ask them about. Then you can get a subpoena or FISA or whatever on the three records. So that'd be an example of a privacy enhancing technology that narrows the transfer of data and it limits the amount of data exchanged to the records that are related to subjects of interest.

A forthcoming blog post that I have is entitled "When risk assessment is the risk" And I think this is missed; there is a fascination about secrets in the data. There's just secrets, there's mysteries. Last time I testified before you, I said, ''There's one in a million things happen millions of a times a day.'' And you could rank and risk score everything. You could actually put everybody in a ranked list and it would actually have everybody from worst, to not worst.

And just sitting on these big lists, actually, is a liability because the moment something bad happens, it was in your list, it was deeper in the list than you could get -- shows that you didn't properly resource. So I think it's really important for engines that do risk assessment, the bar is set so high that it never produces more than the number of resources you have to prosecute it. I think that's really important.

Now, if the risk that you are looking at, the threat, the intelligence, the chatter -- was that there is going to be a kinetic device used in a shopping mall. Then maybe your tolerance in this list of people to go knock on doors, where's your threshold? Maybe it's a hundred. Now if chatter suggests there's something bad going to happen in a big city with something nuclear, maybe -- maybe it's really fair that you would task it with enough people to work the problem – being they would really want to be able to see a thousand deep in the list. So that's my point on the risk-balanced list.

But I think these large lists of rank scores of everybody is not really a -- it's not the best way to go. After something bad happens it tends to make people look incompetent and negligent because it was in the list. And try to explain that. Huh? ''Look at that, on page 4,007 it was right there.''

UNKNOWN MALE: Joe Alhadeff.

MR. ALHADEFF: Thank you. And thanks for the presentation, Jeff. I guess my question goes back a little bit to taking tethering to perhaps the next step. And tethering is useful because it maintains the integrity of the information. If you're allowed to say, ''Hey, the information has changed and we need to know about this.'' One of the main problems which occurs, whether it's between Federal and State sharing or private sector and government sharing of information is, you collected information for a specific use; you now share that information to fulfill, perhaps, part of that use, but how do you know that the information is not going to be used in inconsistent fashions -- going to your consumer surprise -- by the receiving entity or some entity that's three steps down the chain of information that's been shared? And do you see technologies on the horizon that can enable controls to be transferred with the information whether it's, you know, things

like CARML and stuff like that, or other types of controls which may enable some of those data limitations to be transferred along with the data?

MR. JONAS: Well, the best protection of that -- the collection of data, the transfer of data -- it's transferred around a specific use of purpose, but the recipient of it now doesn't fully recognize that scope, and now their scope of use is beyond the original intended scope. I mean, the best remedies for that is MOU and audit.

Despite all the good work being done by many people in areas like DRM, there is a fundamental problem about trying to add controls to the data that transfer from system to system. And the fundamental problem is that you can't really build complex systems where the rule of engagement is everybody has to first re-engineer their system. That's a barrier that is so hard to pass that it will, I believe, prevent that from happening in all but a few scenarios where it is so important to do that. But the more complex the ecosystem the more difficult it's going to be because not everybody is going to be on the same everything and re-engineer all their systems. So I think that'll be a long time in coming for that to be, you know, kind of a service-oriented architecture, a kind of plug-and-play thing that everybody can benefit from.

But there is -- I mean, there is certainly a lot of work being done by a lot of organizations in that area. But I wouldn't hang the hat on that anytime soon.

Is that consistent, Joe, with your thinking -- okay, just seeing if I -- okay.

MR. BEALES: We have time for one more question from John Sabo.

MR. SABO: Yes. Thanks very much. I was struck when you were talking about the casinos, and you paint a picture of a balance, in a sense. You know, you've got a context and they manage -- they see certain threats, and then they see their customers, and then they look at their employees and their own processes. So you paint a picture of kind of a holistic approach to managing this set of things, including, you know -- and managing risk and so on. And -- do they have a model -- a management model? What some of us see in a lot of the DHS programs and Government programs is they'll look for -- they'll look at a particular threat or an attack vector or an exploit channel, and then they'll put tons of resources into figuring out how to, from their point-of-view, address that problem. But no one is looking at this and this and this and this that surround it. So you paint a picture, as I get it, of, like, a context and a whole set of processes that interact. And in the casino examples you used, they seem to have figured out how to pull those pieces together, including customer privilege, customer satisfaction, and freedom, and so on. Do they have a management model for that that you've seen across the casinos, or is that simply something that you're observing and you're making these abstractions? Or do they have a way of managing that more effectively so they balance all these factors at a management level in the casino?

MR. JONAS: So from my experience, that's kind of on a casino-by-casino basis. Some casinos will go out of their way to hire people who have a long history of working

in the area of counter-terrorism. Others will spend -- hire people who have a lot of experience in asset protection and risk management. And these people come with their own processes about, you know, ''What are the different threats upon our infrastructure? What's the threat on our building?'' Some of the casinos have decided to x-ray all the mail. Other casinos have decided to have bomb-sniffing dogs. Other casinos you can't just drive in, park in a parking lot; they will stop you. These are things that are seen as hardening so that if something bad is going to happen somewhere, you can't probably stop it from everywhere, but they want the bad guys say, ''Well, the odds of being successful here are lower, so let's go somewhere else.'' So it's raising that bar. But there's not one set of processes -- there's not one process for that. There's a lot of conversation between the surveillance and security directors. There's organizations where they share their best practices, but there's no set matrix.

Thank you for having me.

UNKNOWN MALE: Thank you very much. We really appreciate your being with us today. It's been an interesting presentation, an interesting discussion. So we appreciate it.

UNKNOWN MALE: Next on our agenda is to hear from a panel of DHS Component Privacy Officers. And if they could join us at the table. I think what we should do is to hear from -- I think what we should do is hear from each of you and then come back and ask questions of everyone. So where we will start is with Lyn Rahilly.

Lyn is the Privacy Officer at Immigration and Customs Enforcement, better known as ICE. She's responsible for ICE's compliance with privacy laws and ensuring that information sharing policies and agreements provide appropriate protections for the information.

Before her position as Privacy Officer, she was on assignment to the FBI serving as the Privacy and Civil Liberties Officer and Special Assistant to the Director of the Terrorist Screening Center, where we met with her a couple of times in talking about Secure Flight, in particular. She earned her Bachelor's degree in Political Science at Mary Washington College and became an attorney after graduating with honors from the George Washington University School of Law. So welcome, Lyn. It's nice to see you again.

MS. RAHILLY: Thank you very much. Thanks for having me here.

I have been at ICE as their first Privacy Officer, April of this year. And I am still learning a great deal about a very large organization with a very varied set of missions and authorities. So I will do my best to answer any questions that you have here today about ICE, but by no means am I an expert on all of their programs and activities at this point.

I just have very few opening remarks just to give you a little bit of background on what ICE does and then what I am doing in establishing the first Privacy Office at ICE.

As you all know, ICE did not pre-exist the Department of Homeland Security, it was created in March of 2003 when DHS was created by statute. It is formed out of the portions of two Legacy agencies, the U.S. Customs Service and the Immigration and Naturalization Service. And it also took part of the General Services Administration, a particular section called the Federal Protective Service. That is also under ICE at the moment. So those three Legacy agencies have come together to form ICE.

ICE has 16,500 employees, and it is the second largest investigative agency in the Federal Government, second only to the Federal Bureau of Investigation. As I mentioned, it has a very broad and deep enforcement mission that focuses on investigations of cross-border crimes and the enforcement of our customs and immigration laws.

In our Office of Investigation, ICE employs Special Agents who work in 27 primary field offices around the country and 50 offices around the world. These Special Agents investigate a broad range of illegal activity. That -- there is a very, very long list. I'll just give you a flavor of some of the things that they do: child exploitation and human trafficking, identity theft, benefit and document fraud, drugs and illegal arms trafficking, cyber, financial, and intellectual property crimes. Every time I turn around in the building I discover something new that they are doing that I didn't know before, so it's a very interesting place to work.

The Office of Investigations also operates a couple of programs you may have heard of; one is the Student and Exchange Visitor Program which operates the SEVIS database. There's a published PIA on SEVIS on the website -- on the DHS Privacy website. It also operates the Law Enforcement Support Center up in Burlington, Vermont, which supports state and local law enforcement agencies which are seeking to find out the immigration status of someone they may have arrested or apprehended. It operates a Cyber Crime Center which supports many of its cyber enforcement activities, including child exploitation. And it operates the Forensic Document Laboratory where documents are analyzed in a forensic fashion.

OI Special Agents also participate in counter-terrorism activity as members of the FBI's Joint Terrorism Task Forces around the country.

In addition to the Office of Investigations, we have our Office of Detention and Removal Operations which enforces the immigration laws by detaining and seeking the removal of removable aliens, which can include illegal aliens or aliens that were here legally but for some reason have now become removable.

In addition, our attorneys in the Office of Principal Legal Advisors actually litigate immigration matters before the immigration courts around the country and the Immigration Appellate Court in Falls Church, Virginia.

In addition, our ICE Federal Protective Service secures federal facilities nationwide. They provide security and law enforcement services at approximately 9,000 federal facilities and screen over 1 million federal employees and visitors entering those facilities every year.

Finally, our Office of International Affairs is the largest international investigative component within the Department. It interacts with the international community through investigations of immigration and customs violations. It also conducts international training and provides support to other countries, immigrations and customs officials, and it helps to guide repatriation efforts for removable aliens.

ICE is much larger than I ever realized when I came there. Just reading that list sort of gives me a bit of a chill in terms of how much I have to learn about ICE and its operations. And it really is just a huge scope of responsibility and a huge number of programs and systems that we have at ICE that my office is gearing up to learn about, assist, and support.

As the first Privacy Officer at ICE, I am very pleased to say that I report to the Chief of Staff of the organization. I am a member of the executive team and my peers are the directors of the offices that I have read to you. So I believe I am properly placed to be effective in carrying out my mission. ICE management has -- from the Assistant Secretary, Julie Myers, to the other directors who are my peers in the organization -- they have all pledged their support for the starting up of my office and any cooperation that I may need in achieving my mission.

Before my office was created, over the last five years of ICE's existence, the way privacy compliance got done was really through the efforts of a number of other offices and individuals and units within those offices who recognized the need to pay attention to these privacy issues and comply with the privacy laws. Offices such as our Legal Advisors Office, our Chief Information Officer -- their IT security unit played a large role in trying to move forward privacy compliance. And also our Office of Investigations had a special unit that really tried to enhance privacy. But because it lacked a central coordinating point, these efforts were often -- although were very well meaning and eager -- often didn't bear a great deal of fruit. Now, with a single point of coordination we have established a privacy compliance process that is documented. Our PIA's are starting to move down the road to approval. We've had one approved so far; we have three others at the Department right now and more that will be coming before the end of the -- [audio ends abruptly].

I'm very pleased to be able to say that the individuals and offices at ICE have uniformly been very cooperative and supportive of the concept of enhancing privacy through our operations. They really do recognize the importance of privacy in achieving ICE's mission, which is a terrific thing. They are very eager to improve on these matters and have been very open to my participation and suggestions and recommendations over the last six months. I can't tell you how many people in the first three weeks I was there

came up to me and said, ''We are so thrilled to have you here finally.'' So it's a very good atmosphere to be building a new office in.

I'm just going to go through a few immediate goals of my office and then I'll turn it over to my colleague, Larry Castelli.

Obviously, setting up the office I need to get additional resources to tackle all of the things that we need to do. I have been given one FTE -- one full-time employee on a one-year detail. And I am seeking to hire another before the end of the month, hopefully. We're also looking at potentially bringing in some contractor support, particularly to address the number of PIA's and SORN's that need to be drafted within ICE. We do have a bit of a backlog simply because my office doesn't have the bandwidth to process all of the PIA's that are currently coming in.

In addition, it's obviously very important in establishing a new office that we make ourselves known within the Agency and raise awareness. Along those lines, we have established a website on ICE's internal intranet and put a great deal of content on there. And we found that that's been very helpful to individuals and really understanding what it is we do and how they can interact with us.

We're also going to be working -- as Hugo mentioned -- to update all of our Legacy SORN's by the end of this year. We have, as I said, several PIA's in the pipeline -- one approved. My goal is to have five or six approved by the end of 2008.

And in addition to that, we are currently working on a project to enhance our privacy incident notification procedures and remedial activities within ICE; this is the data breach process. Shortly after I got there we set up a working group that meets every other week between myself, our IT security folks, and OCIO, and our Internal Affairs Division. And we are working to ultimately draft a set of procedures within ICE to make clear what everybody's responsibilities are in the data breach process.

And finally, one of the other initiatives we've been doing a great deal of work on is to draft some enhanced contract provisions to include in new and existing contracts at ICE to ensure that contractors are obligated to also participate in the data breach notification process with respect to any federal data that they may hold, and to provide for enhanced physical and technological security protections for the data that they may hold that is federal data and PII.

We also hope to change the way we actually solicit contracts to have contractors, in their proposal, explain to us how they will comply with Federal privacy laws so that that can be part of what we consider in comparing bids on a particular proposal.

So with that I will turn it over to Larry.

MR. BEALES: Thank you, Lyn. And welcome to Larry who is the Privacy Officer of the Customs and Border Protection.

MR. CASTELLI: Thank you, Lyn. And thank you very much to the members of the committee for having me here.

Previously, my Executive Director, Sandra Bell, has addressed the Committee -- I believe it was several years ago about the time I was first established as the Chief of the Privacy Act Policy and Procedures Branch at CBP, which is a rather long title for basically a Privacy Officer. But that's kind of how we've done things.

Privacy at CBP grew out of what was the Disclosure Law Branch. At one time we had a combined FOIA and privacy practice. As time grew on we discovered that there were increasing demands from both compliance concerns from both the FOIA as well as privacy. And so we created our privacy branch in 2005. And since that time, what we've tried to do is get on top of privacy at CBP in a more proactive way. And I say that simply because CBP has long -- or not long -- I mean, CBP, like, as Lyn noted about ICE -- CBP was created on March 1st, 2003 as a result of the standing up of the Department of Homeland Security. We were formed principally from components of the Immigration and Naturalization Service, most notably their inspection service as well as the border patrol. And we were composed of components of the former U.S. Customs Service, principally, their inspection and non-investigative functions. We have worked very closely with -- and we still do work closely with ICE. For instance, the Office of Investigations does investigate many -- well, actually all of the crimes that we would identify, all of the civil penalties that we would identify that would require investigation are referred over.

One of our -- I would -- I could give you a larger overview of what CBP does, but suffice it to say that CBP is your border agency. We are either through our 300-plus ports of entry where you can officially enter the United States, or just through the land border itself and the -- and sea border where the Border Patrol -- between the ports of entry patrols, and technically you're not allowed to enter. In that, irregardless -- sorry, regardless of whether you're a U.S. citizen or not you must still cross at a defined border port.

What I wanted to focus on, though, and in keeping my marks somewhat brief so that there be time if you have questions, is the privacy challenges that being a border agency present. As Hugo noted and as Lyn noted, one of our first and foremost challenges is working with DHS to update our existing System of Records Notices. The Privacy Act very graciously created the concept of a System of Record Notice as a way of telling people what's going on. Frankly, I know lawyers who can't figure out what they mean. So it's not necessarily the most perfect device; however, if you can do better at explaining what's going on -- and one of the tasks we have taken at CBP is in reformulating how you describe the data. And what I mean by that is -- many of you may be familiar with a Legacy System of Records Notice that we have out called the Treasury Enforcement Communication System. TECS is in the process now finally of being revised to be a new DHS system. And in that process it is being narrowed in terms of its scope. One of the reasons for that is -- I think as Mr. Jonas noted -- you have this idea

that you want to avoid customer surprise. The government has customers, they're also called citizens, and we need to let people know more about what they can expect when we collect information from them.

CBP has gone through a number of challenges as it has broken portions of TECS out and created separate Systems of Records Notices. In an effort to try to give more transparency and in an effort to try to redefine these data sets in ways that would allow the public to know more about what's happening, but yet at the still time permit CBP to do its principle functions. And CBP's principle border mission is part border security and part trade facilitation. And I think it's important to remember the trade facilitation part because, you know, there was a time years ago when it was the Customs Service, and what we looked at in cargo was basically what's in the box. Now moving forward what we've determined is, it's no longer simply a question of what's in the box; it's also a question of who touched the box. And so as we go forward, what we see are that even our commercial systems which previously we only thought dealt with business confidential information, extensively privacy to a business entity, now deal both -- with both. There are mixed systems now. It's not only trading secret data, it's also personal information about the persons who work there, who are supplying the data, who are carrying the data.

So our challenges are partly to update our systems and in the process create more transparency to -- I don't want to seem glib -- but, in some ways to better message what is happening, what that systems has, what's in it, in some ways, how you can actually get that information. Much of what CBP collects -- certainly in the commercial area -- is available to the submitter of that data. Increasingly in the personal area -- if you look at our systems like the Advanced Passenger Information System, or even if you look at the Automated Targeting System in terms of the passenger name records that we collect there. We have made efforts to make that information accessible to the individual or to the person, if you'll forgive my distinction, simply. Privacy Act makes a distinction about persons and individuals; DHS by directive has chosen not to, and CBP embraces that directive and attempts in all systems where we have mixed use, where we collect information from foreign nationals as well as U.S. persons, that we give them equal rights to access.

Part of this also is -- and part of -- a large part of my function lately has been in regulatory compliance in the sense that with the new initiatives that CBP approaches, the Western Hemisphere Travel Initiative, the ESTA Initiative which was the Electronic System for Travel Authorization, enhancements to expanding the Advanced Passenger Information System to general aviation, or you might know them better as private pilots. Or even the more recent regulatory proposals regarding the security filing, sometimes referred to as 10 + 2.

All of these regulatory initiatives require now privacy compliance in conjunction with their proposals being rolled out. As a way of explaining to people, 'What are we going to collect? What are we proposing to collect?'' And now, also, ''What are we going to do with what we're going to collect?'' And ''How are we going to protect your data?'' and ''How can we assure you that we're using it for a particular purpose?'' And I

think -- and the last thing that I would talk about just now is using for a particular purpose and how we us it, is probably the biggest challenge that CBP has right now, which is sharing data.

We -- you know, yesterday we took a tour of that fusion center for Las Vegas, and I think one of the issues that came up at some point is there were several questions that were raised about, ''What data can you access? Who has access to what information? Are there rules? Are there guides? Are there limits on how that information can be used?'' Information sharing is critical in terms of allowing different data sets to be compared to allow the information that may not reside in one data set to be combined with that information so that someone can know more or someone can know better. The problem with sharing data is you can't share it all. And I think in what we've tried to do through a variety of different vehicles using Memoranda of Understanding, using Memoranda of Agreement, is to create a framework or a fabric where governments can share, where federal and state and local can share, and to create ways and means whereby the information can be shared. I mean, we even have agreements now. You know, if you look at the development of the automated commercial environment, the sole purpose of the International Trade Data System is to create a portal for the Federal Government to share trade data as it relates both to enforcement and also to compliance. And in enforcement you're getting into the issues of import safety.

But I think that's -- information sharing becomes a very critical challenge because we don't want to share everything. We want to share what you need. You know, The Privacy Act defines that in the concept of ''need to know.'' So, you know, so you need to have this dialogue back and forth where you're asking, ''What is the use? Where is it going?'' And, you know, to go back to that issue of customer surprise, an agency needs to know what further dissemination may or may not happen with the information it provides. And so that tends to create further feedback loops. But these are the -- I think, principally these are the larger challenges that we face.

Separate to that is also always keeping guidance up to speed. And our continual training efforts that we do, we plan four to five training sessions a year around the country for CBP officers to reiterate principles of data security, to reiterate the procedures whereby they can request permission to share information with state and local, to facilitate investigations, to facilitate other compliance efforts. We also have several training -- online training systems that we use that officers and employees must pass in order to maintain access to systems. This is good primarily because it reinforces. It reinforces the knowledge of what the protocol is and what the procedures are for sharing and for safeguarding the data. And as with anything, the more frequently that you remind people of what the procedures are the more likely they are to stick to them.

I'll leave it at that and defer to my colleague, Donald.

UNKNOWN MALE: Thank you very much, Larry. Our final speaker is Donald Hawkins, who is the Privacy Officer from the U.S. Citizenship and Immigration Service. He had served as the Assistant Disclosure Office for the United States Secret Service; I

like that combination -- the disclosure of the Secret Service. And prior to assuming those duties, he performed as the FOIA Officer at the Office of Management and Budget. Welcome.

MR. HAWKINS: Thank you. And thank you for having me. Again, my name is Donald Hawkins. I am -- at the Privacy Office at USCIS, I am a direct report to the Chief of Staff. Upon coming to CIS, of course, I was -- there was a learning curve there in terms of all the different jargon at CIS opposed to some of the other components that I worked at.

But there were four main things that the Chief of Staff had brought to my attention that he wanted taken care of right off that bat, and that was our PIA's, our privacy documentation. CIS had 102 systems that were delinquent. So the PIA's and SORN's and then PRN's were the main target of tasks that had to be done, had to be taken care of.

The second one, they wanted some policy guidelines to establish at CIS in terms of how are we going to handle PII within CIS? CIS is 99 percent personally identifiable information. They deal with the benefit application from dealing with aliens from the initial application submission all the way to citizen naturalization. And through that, there are many applications that are submitted, and there are just a ton of personally identifiable information that is submitted to CIS.

After the policy development, the next stage was to establish the Privacy Office. That meant I had to hire someone to help me to get all of the privacy documentation done and also to advise the Director and executive staff as to how the privacy program would go forward.

And the last step was the training. We wanted to develop a robust training program so that we can educate our staff so that they, not only would just be responding to mandates or memos, they wanted a detail as to actually how we do it.

And going back up to the PIA, the very first step, coming in, we had 102 PIA's that needed to be worked. Today, we have about four of those PIA's that are still pending. Step back -- we have those eight of those are pending. Myself and the Deputy who came on in July, we have robustly worked on these PIA's and all of these other privacy documentations and have worked with the Privacy Office as well as the respective programs to get these PIA's and other privacy documentations completed.

The Privacy Office at CIS was actually established July 12th. Myself, I came in July -- I mean, November the 12th of 2007. We've currently interviewed or have interviewed several people for an administrative position, and our goal is to try to get the Privacy Office staff up to six or seven. That's our goal.

In terms of training, we have put forth a robust training program with which we submitted to the executive staff that would include everybody, including executive staff

all the way down to the lower line employees. Myself and the Deputy have gone out, we have traveled abroad, have trained staff out in the regions direct -- I mean, the district office, some of the field office. We have sent out directives, policies, PII guidance to the staff to ensure that they know what they are supposed to be doing when they are handling all of this PII information.

Coming in to CIS and talking with a lot of the staff and talking to a lot of the managers, it -- had them understanding that many of them didn't have any idea as to what PII was. And that was our number one goal was to educate our people. And we have gone out, and, I mean, robustly approached our staff, approached our managers, and explained what PII is, what it isn't, and how we're supposed to handle it.

In terms of my goal for the program, I would like to see the privacy -- CIS privacy program to eventually get to the point to where we can grow or get enough people where we can actually go out and do live training. We will be doing CBT training; we also will be doing WebEx. But eventually we would like to be able to have enough people where we can go out and speak with the people in person -- not extending two or three people well beyond, you know, their abilities. We will have to be able to grow.

And in terms of this -- the management, they have totally bought into the Privacy Program. I mean, I have total support. CIS Privacy Program have grown tremendously in the short time that I have been there. And I am very happy being there, I am very happy in the direction that we are going, and I can see in the future that CIS will be a premiere component in terms of how privacy is done and, you know, and in terms of the overall reporting of privacy. I think we're -- plan to have everything done by the end of the year.

And that's all I have.

UNKNOWN MALE: All right. Well, thank you, all. Questions from the committee? I guess we will start with Joe Alhadeff.

MR. ALHADEFF: Thank you. And I guess this question may be fair game for everyone to answer, but I guess it was sparked by Mr. Castelli's comments. So I guess I'll direct it, but it's not particular. And it really goes to some of the concepts behind architecture. So when we think about some of the architecture of systems and choices that are made, and it builds a lot of Jeff Jonas' comments about, kind of, the customer service paradigm. Two things came up; one was the idea that was raised as a question in the fusion centers about the sharing of information, and from an architectural perspective, I completely understand the need to share, I completely agree that the sharing has to be done to accomplish the purposes. The question is, sharing inside a fusion center is not really that much of a question, but sharing across systems becomes a question because those systems aren't architected to the same degrees the awareness of the people using the systems is no way consistent. And there's only so far you take that with an MOU between the organizations to actually understand how that's happening. So a lot of those state and local systems may not have a PIA, may not have a training program related to

privacy; and even if you have the most well-intentioned purpose and the most well-intentioned employee, may still end up with data use that would be a surprise to the customer, or the citizen in this case. And those are issues where I wonder if there has been thought about how to look at the architecture. And also when looking at those -- and, you know, when we look at PIA's, the PIA goes to what is the legality of the sharing and how do you establish that? But I wonder sometimes if part of the concept in terms of, do we do a risk analysis on the PIA as to evasiveness -- invasiveness and effectiveness, because we really don't figure out if there is perhaps a least -- a less invasive option that might be equally effective where you can engage in the trade off. And that also goes to usability. And so I think some of those factors probably have to become part of the evolution of PIA's, especially as PIA's go from system PIA's to ecosystem PIA's, because now you're going to have to think about the PIA as it goes through or across the information life cycle.

And I know that none of the folks on the panel are in a position to control this dynamic across their organization, but I'm just wondering if there is thinking in the organization about how to deal with some of these extended issues.

MR. CASTELLI: Can I say yes and just leave it at that? No, I'm -- yes. There is thinking, and it's, you know, it's interesting because, you know, I look at things like a fusion center and I look at, you know -- and a fusion center at some level is simply just the next step along the evolutionary path from formally what we used to call task force, or when you would have multi-disciplinary enforcement teams where you'd perhaps have state and local working on a drug case; you'd have state and local working with federal; and you'd have multiple jurisdiction and everyone would work together. And the theory was always that everyone would bring their own information into the sort of circle and they could share with one another there because it was ostensibly still under the control of the individual who was bringing it. And as long as you had an asset, an officer, as ong as he or she were part of that, that sort of sharing circle, there wasn't a problem because arguably they were still controlling.

The other thing to remember, too, is it was paper. Paper, although you can photocopy it, it's a little easier to control paper -- and from an architecture standpoint, I mean, I will defer somewhat to the IT people on how that gets done. I mean, the concern that I've always had is -- and what I've always tried to [inaudible] in to the MOU process at CBP, as much as I've been able to control it, and increasingly because of the way we've written our PIA's to require MOU's whenever you're sharing outside of DHS -- or something we call facilitated access.

And just to clarify, facilitated access means you don't have an MOU, but it means you're practicing Mother May I. And Mother May I is you're preparing a -- something in writing, a written request -- and writing in this day and age can be, you know, on cellulose, it can be an electronic media; it really doesn't matter, it just has to be something that is somehow tangible. But you're making a request that says what it is you want, why you want it, why you -- you know, not -- and I say want, I mean, technically, it's why you need it, what's your authority, what purpose you're putting it to. And it

gives the agency that is in possession of the information the ability to review that and make sure that it is [inaudible], sharing would be consistent with the purpose for why it collected the information, the purpose for why it shares information generally, the kinds of objectives it seeks to accomplish. MOU's tend to do this on a much broader basis and allow for a little more regularity. But we do try to include those limitations. And so, what I guess my answer on the architecture issue is, I would like to see architecture that does in fact inhibit -- what I would call third-party sharing, which is the sharing outside of that initial circle. I mean, all I can contemplate is that circle. And so maybe you can't bring it in to other systems, maybe it has to be coded so that it can only be read-only in a particular system.

MR. ALHADEFF: Just one follow-up, because, I mean, the questions were all appropriate questions to should the sharing occur, except there were a couple of questions that we're missing, which is how do you control it, how do you dispose of it, who might you share it with, who are you allowed to share it with? Those -- is that part of the MOU process also? Because if you don't know those things, then the custody of the information is at risk.

MR. CASTELLI: It -- that's not typically a question so much as that is the condition under which you're receiving. In other words, like, if we do an authorization, you are basically -- the terms under which you are permitted to have access are you're going to only use for the stated purpose in the document. If you gave too narrow a purpose, you're going to have to come back for a second request.

Now, we often advise -- and there's a lot of verbal communication when you want to clarify what exactly it is. The MOU's do the same thing. They typically contain what we call a confidentiality section. The point of that is to remind them that the information was collected by CBP. That it remains a responsibility of CBP to ensure it's safeguarded in that vein; that responsibility is now also shared by the receiving entity, and they must protect it the same way CBP protects it. And CBP reserves a right to audit that, and if they don't then we would seek to stop sharing.

In the onetime instances, we typically provide the information in hard copy often and in those contexts, again, we remind them it's only for a stated purpose. I mean, much of this is if they choose to seek forgiveness rather than permission on their further use -- I guess your next question is, what happens? There are agencies that don't get information from us. I've shut them down and I've told them, you know, that there's nothing else that can be done.

Now, there's a way to rehabilitate yourself, obviously, but, you know, if you don't use the stick then it's not worthwhile to have a stick.

UNKNOWN MALE: Lisa Sotto.

MS. SOTTO: Thank you all very much for joining us. Lyn, when you were speaking about the breath of your organization and the sheer number of the people in the

organization, it occurred to me that training and awareness is probably very difficult because you have different levels of folks; you've got the management folks, you've got the folks who are really at heart law enforcement officers, and I would think there's a real diversity of interests throughout the organization.

Larry and Don touched on training and awareness. I think both are so critical and very different training on existing policies and procedures versus awareness so that to the extent that new practices are coming to the [inaudible] like reasonably new laptop searches at the border or new architecting of systems, developing of systems so that that privacy has to be built in from the start.

How do you really make privacy something that folks think about all the time in thinking about new practices -- really more awareness than training? And how receptive are the folks in your organization to privacy? And I would direct this in particular to both Lyn and Larry.

MS. RAHILLY: Well, obviously, I mean, training and awareness is critical to the success of any program. I was very pleased when I came to ICE to find out that the Information Assurance Division in our Chief Information Office had preceded me in terms of being established and really beefed up in resources by about a year. And they have an annual requirement under FISMA to provide information assurance training, which I took within the month I was there as it was required at that time. And I was extremely pleased that they had integrated a great deal of privacy content into the Information Assurance training, which I think is -- it was a very smart thing to do.

I will be working with them next year since it is mandated for every individual, every federal employee, and I believe every federal contractor that has access to a federal IT system to take that training. I do plan to enhance some of the privacy content in that training in order to boost what they've already done, which is very good, even higher.

I have been doing a bit of reading about training, and one of the things I do get a little concerned about in the area of training and awareness is over-training people. You know, we all now have these online, virtual universities -- I'm sure in the private sector it's similar -- but in the government it's very popular and every year you get your litany of required training, your EEO, and your ethics and your information security training and all of that. And I've been reading some articles about, you know, studies that have been done on effectiveness. And I think it's important to try to integrate training into existing training as much as you can on privacy. I'm starting to doubt how effective truly standalone privacy training may be versus privacy training that is integrated into other existing training that may be job specific, to, for example, our special agents. It may be generic training that everyone has to take, like the FISMA training. And I think I'm going to be looking at that as a path forward on the training front. It's different than what I did at my previous job, but I had an office of 300 people; that was the size of my program. I trained every one of them individually and they sat there for an hour and listened to me talk about privacy. So I obviously can't do that with 16,000 employees, and so we'll be taking a different tact.

On awareness, you know, I think that's a different issue. And I've really been hearing a lot about what Peter Pietra has been doing at TSA. I don't know if he's shared some of his exciting privacy posters with all of you. Have you seen the comic book type -- what is he, Privacy Man? He's Privacy Man. And he and his sidekick, Anthony Johnson in the Privacy Office are -- they really did a great job with it. I encourage you to get some copies. And, you know, they've put things like that up. I think things like that are very helpful.

I am really waiting to get a little more acclimated at ICE in order to find out what I think will be the most effective way to reach people. I really do think it's so different in different organizations. I don't like to charge in and simply put something out there that may not be the most effective way to go. But it is something that after I think we finish our first year we're really going to be turning some of our resources to doing.

And, again, I would like to have a more tailored approach to reach the people within the context of their own job so that it's more meaningful to them, and perhaps have more specialized content that reaches them directly.

MR. CASTELLI: I echo what Lyn's saying about the training. We actually at CBP -- I mean, CBP has roughly 50,000 employees now, and we do both what Lyn has suggested -- she's right about specialized privacy training. If you roll it out to everyone, it becomes sort of background noise at some level because it's not particularly tailored to what they do. What we do typically is we have computer-based training; we have two courses, a general privacy awareness course and a specific TECS privacy awareness course. And anyone who wants to use an admin or mainframe computer system must pass one or both of these courses. Actually, the general privacy one isn't a passing, it's just taking. But you must pass the TECS privacy awareness if you want access to TECS. And in order to access any law enforcement system in CBP you must first have access to TECS. And so there's a layered approach to building on what your knowledge is. Both of those computer courses contain a number of vignettes, I guess would be the best way to put it, where you -- circumstances that would come up in the daily life of an inspector working at the border, instances where someone wants to know something about their neighbor or something like that, and what are the correct answers, what are the choices, what are the choices you're confronting, how best to analyze it. I mean, we've had instances, you know, or other -- and another vignette deals with persons from another agency wanting information that may or may not be -- they were told by the President to come get. There's still a procedure and it lays out what that procedure would be.

The specialized training we typically do is to those individuals at the various field locations and at headquarters who on a more regular basis are points of contact for routine sharing of information outside of CBP and DHS. For them, we believe it's important to give them more information about the -- what we have, how we use it, what our authorities are, and the best way in which to do this. We also like to share information with them about who their colleagues are who are similarly situated. Give them -- so that we can create informal networks so that people can understand. One thing

I find is when you create networks like that, people find out when people are, what we call port-shopping -- ‘‘They wouldn’t give it to me in Houston but I understand New Orleans is easier.’’ You know, we try to avoid that.

You know, the other thing is, we have looked at and we do have part of the basic inspector course, or it’s now I think the basic CBP officer course. There is a portion that deals with privacy awareness. Because of what CBP officers do, the role they play at the border, the role at primary when they’re first encountering individuals as they cross, the role they may play at secondary where they may be clarifying a match to a database that was a misidentification, or where they’re simply clarifying information that’s discrepant, or maybe they’re performing a random search of baggage. Or perhaps there was an actual match that was appropriate and they’re doing a further search in that regard. In those contexts, the officers have already had -- the basic training courses is 12 weeks down at the Federal Law Enforcement Training Center in Glynn Co., Georgia -- Glynn County, Georgia, in Brunswick, actually. There are daily [inaudible] that provide them with information about current threat situations, current topics of concern regarding what we might be looking for. There are also alerts that are available online.

One of the things that’s always drilled into them is that there is a code of conduct, there is an expectation of professionalism on the part of the officers. What reinforces that is also a discipline system that is very quick to issue discipline and to punish where you violate that. An example -- I mean, if you look back in the Customs history of CBP, in 1998, then Commissioner of Customs, Ray Kelly, in response to concerns about perceived racial profiling in passenger processing, implemented an independent commission -- a three-person independent commission to review the entire passenger search policy and make recommendations as to how that could be revised and updated to be more neutral on race and other issues.

The CBP constantly tries to review what it does in these areas, in part because it -- I mean, you know, it’s a public relations issue but it’s also -- what I’ve often tried to explain to people, the bigger problem for CBP is you have all these people crossing the border, only a few of them are actually persons who really should prompt your law enforcement interest. And it’s how do I identify which few that is?

You know, just -- you mentioned laptops and one of the things I did prior to coming down here, I got some statistics on that because I know that CBP doesn’t typically keep a lot of statistics on the searches it does, although any time you go to secondary, there’s a report that’s filed by the inspector at secondary documenting that interaction. And that is something that is available through FOIA because it contains a mixture of official and factual information, it -- you would have to use FOIA.

But between August 1st and August 13, for instance, 17 million people were encountered by CBP at primary. Of the 17 million people, roughly 320,000 were referred to secondary. And of that, in the case of laptops, 40 were inspected. And that turned -- anything from turning the power on to actually looking more specifically at the hard -- you know, contents of the hard drive. So that’s a very steep compression, and, you know,

and it's the sort of the thing, like other types of invasive searches, there's a continuum that the officer must follow. It's not simply, you know, ''It's a bad day, guess what?''

And so I think, you know, it needs to be something that people understand is it's necessary; it's necessary because Title 8 requires it for evaluating someone's admissibility into the United States; it's necessary because Title 19 requires it because of the various laws that we enforce.

Lyn mentioned cyber-crime and, you know, one of the cyber-crime issues we look into is pornography -- child pornography, in particular. And so that's -- we must -- we make referrals regularly on that basis. Well, when they happen. But anyway, that -- so that's, I think, just to give some context of the sort of -- the full environment.

MR. ALHADEFF: So how many of the 40 laptop searches turned up anything?

MR. CASTELLI: I don't know exactly how many. The statistics I got were just in -- they were just pulling the -- they just gave me some quick stats before I came down, because I had asked them, I said, ''Well, what do we know about it?'' I don't know. Many of them, I don't know -- I don't even know if Lyn would have any information about it because I do know that a lot of that we share with her. But I don't –

MS. RAHILLY: We do have a record of how many are seized, which of course is a Fourth Amendment probable cause seizure. There is a database that actually CBP and ICE both use to document any seizures, be it if it's a laptop or, you know, a piece of -- a good, piece of merchandise. I don't have -- Larry got those statistics independently so I wouldn't be able to tell you of the 40 how many were. But one of the things that both of our agencies are doing in response to the interest in the laptop search issue is to begin to collect more data on this. And that effort began just very recently. So we do expect in the coming months to have more data.

MR. ALHADEFF: That's good. I mean, the compression -- the compression is good that it's not in a lot of -- it's by far not most of the laptops. But the other question is, how useful is it? And that, you know, that's what this statistic would really go to, it seems to me.

MR. CASTELLI: I suspect one of the things, because I do know Lyn is right, there is a concerted effort to develop more metrics to track what's happening. And whenever you do that, part of that is that efficacy analysis that follows on, what did we find? And then how useful was it?

MR. BEALES: Richard Purcell.

MR. PURCELL: Thanks, Howard. I'd like to turn our attention briefly to the structure in your divisions or components. For the Privacy Office -- Lyn, Don -- you stated clearly that you report to the Chief of Staff. You've had to -- Larry, less clear and, you know, somewhat troubling I think for a number of the members of the Committee

that components of the Department haven't necessarily embraced the strong and robust and, kind of, clear structure that we might otherwise prefer. So can you talk to us -- all of you, if you would -- about the structural -- the way you've structured your office or the way your office is structured within your component and what efforts, if any, are under way to change, alter, or strengthen those structures.

MR. CASTELLI: Well, since I gave the least information, I'll start. I have a staff of nine attorneys who work for me, and we are a -- we're in a legal office, basically, the Office of Regulations and Rulings is part of the Office of International Trade. And primarily we're situated where we are because that's where the FOIA and privacy function has always been situated. And CBP, or Customs prior to that, much of the legal regime of CBP came from Legacy Customs, and so it follows that.

Just in terms of mapping out what the chain of command is, I report to a Division Director who is the Division Director of Regs and Disclosure Law. My Executive Director, Sandra Bell, is the next in line; and then I have an Assistant Commissioner; and then the top management of CBP, the Deputy and the Commissioner. Separately, I have direct access to the Chief of Staff for the Commissioner as it relates to taskings that are privacy specific. So if I need to, I can reach out to him to basically -- if we need to promulgate information agency-wide, I can reach out and use that avenue to get the message out. Inquiries to CBP that come through the Chief of Staff's Office are directed to me.

What we've done is, in addition -- I don't want to say informally, but basically networking within the Agency, you know, I've made outreach efforts to -- for instance, our Information System Security Officers who are the -- a large part are contractors but work for the Office of Information Technology. And they are, in terms of IT development, they are the people who are first coming up upon security requirements and privacy requirements that FISMA would require for large IT systems. We have a representative attend all of their sort of weekly bull sessions, for lack of a better term, just so that there is someone who can provide advice to them about what are the privacy concerns that they need to be aware of; more importantly, to have someone available to answer their questions.

I -- CBP has recently developed requirements boards for some of its larger systems, and we placed a privacy representative on each of these boards to, again, essentially to be an observer but also to advise on the privacy issues as initial requests come in, as you look at development. This is true for instance for the automated targeting system. And it's an effort to sort of get on top of -- to achieve that initial intent of the Privacy Impact Assessment, which was to make privacy part of the initial determinations as you're going forward. That hasn't always been the case, but I've attempted to leverage some of the process that we've had with regard to public feedback on some 20 of our systems to say there are better ways. And, you know, we need to grow and evolve the same way we anticipate our systems will. So, I -- that's –

MR. BEALES: Ramon Barquin.

MR. BARQUIN: If I recall -- [speaking off microphone].

UNKNOWN MALE: Did you have a follow-up, Don? I'd be happy to hear structurally what your areas --

MR. HAWKINS: Yeah. At CIS, I am a direct report to the Chief of Staff. I also have direct -- or a direct line to the Deputy as well as the Director. I mean, we have senior leadership meetings every Thursday. I mean, any time that there is any privacy issues or anything regarding privacy that needs to be disseminated above my pay grade is -- can easily be done. Now, there are no restrictions. They have opened the doors to everything that I need, so, I mean, it's a good program to be in. It's wonderful.

I mean, they bought into the program, they are very supportive, and I don't see CIS having any problem with dealing with privacy in the future, at least with the current administration.

UNKNOWN MALE: I --

MR. BEALES: Okay. You have five minutes before the tape runs out.

MR. BARQUIN: Hopefully this is very quick. I seem to recall that at one point even though there was not a statutory requirement that Homeland Security -- the Department overall -- had decided that it would also extend all of the privacy policies, principles, et cetera, to non-U.S. citizens. And I just wanted to make sure that that is correct, and whether there is any different –

UNKNOWN MALE: Yes.

MR. BARQUIN: Okay, good. Then, where there is any differentiation vis-a-vis legal residence and illegal.

MR. CASTELLI: In echoing Hugo, yes. Hugo issued that directive and we follow it. The -- no, we don't make a distinction between legal or illegal. We've -- we interpreted the directive on mixed use systems to basically say, much like the FOIA law -- you know, 5 USC 552 says, ''person.'' We're not looking at your nationality. We're basically -- when we're looking at the administrative grant of access and amendment -- and, you know, let me clarify that the directive governs departmental policy and so to the extent that the rule in the Department is you get access and amendment, that's true. Legally, if you were to go into court, I suspect the court may look more precisely at what The Privacy Act itself says. Our hope is that by providing the administrative right you won't need to go to court for, you know, to seek expungment or something else. But we don't make a distinction; we basically have -- and since -- as long as I've been with -- in the program and have been pushing for it, I've tried to take the approach that if you gave us the information we believe you're entitled to get a copy of what it is you gave us back.

But just what you gave us. I mean, if we -- you know, we would reserve the right to look at it more closely if we marked it up or something.

MR. BEALES: All right. Well, I want to thank all three of you for being with us. And we can pause to change the tape. And then we will move to -- oh, maybe after the tape change before the subcommittee reports, I think Hugo wanted to say something briefly about the role of privacy officers in the Department. Okay. So -- pause.

MR. BEALES: Okay. We can resume. All right. Hugo Teufel.

MR. TEUFEL: I just wanted to mention to the Advisory Committee -- I wanted to talk to the Advisory Committee a little bit about Component Privacy Officers, and I gather that informally the Advisory Committee has been made aware of the things that we've been doing at the Department with respect to Component Privacy Officers. But I just wanted to talk about that on the record as it were to the Advisory Committee.

Up until last year, the Department, beyond the Privacy Office, it had two or three people or officials who were considered Component Privacy Officers. So you had at US-VISIT, a Privacy Officer; Transportation Security Administration there had been a Privacy Officer, and over at NCSD -- which is I think National Cyber Security Division -- Andy Purdy had been the Privacy Officer. Andy left the Department, and NCSD had not replaced its Privacy Officer. But we had Privacy Officers at TSA and US-VISIT.

And of course what we found by and large was when you had folks who were Privacy Officers at Components, the quality of the privacy documentation came from the Components was much higher. And while privacy documentation typically is an iterative process, with Component Privacy Officers you were looking at maybe a couple of drafts and maybe a couple of months at most to get a PIA or a SORN through -- I'm talking your average Privacy Impact Assessment or average Systems of Records Notice. With Components that didn't have Component Privacy Officers, sometimes it could take months or years to get privacy documentation out. That's just one aspect of what it is the Component Privacy Officers do that makes them so useful at the Department. And of course, as we all know here in the room, its information and often it's personally identifiable information that is the key factor in the Department's Components carrying out of their missions. And so in looking -- well, so let me back up. Prior to GAO's report on the Privacy Office last year, my office had been looking at where we should have further Component Privacy Officers. So we had been working on it prior to GAO issuing that report; the report suggests that there ought to be Component Privacy Officers. And I don't recall the exact language of the GAO report, but I seem to recollect that the language was fairly broad and perhaps might suggest having Component Privacy Officers in every one of -- arguably, every one of the 25, 26 Components within the Department. We looked at that and said, you know, ''It's not practical.'' And some Components would have push back if we were to say, ''Well, we need to have 26, 25 Component Privacy Officers in the Department.'' So we looked and said, ''Where are the areas where, either because of the amount of personally identifiable information or because of the sensitive nature of the things that the Component was doing, would it make sense to have Component Privacy Officers?'' And so I wrote to the Secretary last year and made

a set of recommendations for Component Privacy Officers, and the Secretary agreed with me and late last year signed off on my memorandum saying, ''Yeah, good idea. We ought to have Component Privacy Officers at six selected Components for operational II department level.'' The Department level Components, Science and Technology, the -- and Intelligence and Analysis, and then the operational components would be CIS, ICE, CBP, and FEMA.

And so as a result of that, the components have with -- some with alacrity and some with all do deliberate speed have been moving forward on selecting Component Privacy Officers. And so that's how we've gotten to have all the folks who are back here who will be talking to you today -- the three that have talked to you and then the others who will be coming up to talk to you later.

So you need to have -- I think you needed to have that context more formally and on the record to understand why are these people here talking to you today.

MR. BEALES: Okay. David.

MR. HOFFMAN: Just one quick comment, Hugo. I'd like to just officially commend the Privacy Office for taking the [inaudible]. That was a key part of recommendations that this committee also had made to your predecessors. To take those actions it's, I think -- now, those of us who have played the similar role in the corporate environment have found it's the best way to make an impact of operationalizing privacy across a broad organization, and I'm really looking forward to -- I think the promise you've made is incredible and greater than I thought was going to be able to be made in a short period of time. And I'm looking forward to now seeing the building out of that organization, the tools you're going to be able to make available to Component Privacy Officers to help them do that job and operationalize the privacy controls in each Component.

MR. TEUFEL: Well, thank you. Where we've brought on Component Privacy Officers -- or where we're bringing on Component Privacy Officers, and really in a very short period of time you're seeing substantial improvement in compliance and documentation and advice to the Components. And so I don't want to single anybody out because they're all great. So, thank you.

MR. BEALES: All right. Thanks, Hugo. Time now for subcommittee reports. And I guess we will start with Privacy Architecture. Jim and Joanne.

MS. MCNABB: Thanks, Howard. Okay. The Architecture Subcommittee has handed out -- and here is another copy if anybody in the audience wants one, there must be more, but there may not be.

A proposal for adoption by the Full Committee -- this is something we've been talking about at several meetings, and it's a very modest but important step in the direction of requiring applicants for State grants from DHS to consider the privacy

impact of the grant proposals that they are submitting. We're not totally clear whether in a current stage of the grants award process whether this can have any impact on this, the round that's under way right now. But –

UNKNOWN: We remain hopeful.

MS. MCNABB: -- we remain hopeful. And in addition to asking you to approve this, we would ask you to approve urging the Privacy Office to push this through as rapidly as possible.

And so what we are proposing here is that applicants for the grants to States answer, essentially, the questions in the office's privacy threshold assessment. And it's basically questions designed to identify whether or not the proposed program would collect personal information. That's it. The questions are: ''Would the project collect, generate, or store information on individuals excluding information used to administer the project, such as payroll information?'' So it's really outside, not employees that we're asking about. ''Would it collect any of the following: Social Security Numbers, other numerical identifiers such as account numbers of driver's license numbers, biometric identifiers such as fingerprints, DNA, iris images, facial scans, or any images or recordings of individuals?'' And then, ''Would the project collect, generate, or retain any other information about individuals?''

Then we would say, you may be required to prepare a Privacy Impact Assessment or a similar documentation upon award of the grant, just, you may be. We would -- we think at the very least this could generate some good information on how many of the grant projects actually do collect personal information, which isn't something anybody seems to know at this point. So our request is that the Committee approve this recommendation to the Privacy Office.

MR. BEALES: Questions or comments? Jim.

MR. HARPER: I just want to say briefly that Joanne has done great work to carry this project forward over the course of more than a year. It was a year ago, I believe, that we talked about this and talked about inserting language like this into the grant making process. A year ago, some bureaucratic snafus apparently prevented getting communications to them timely and so I would like to second [inaudible] make part of this our strong encouragement that the Privacy Office carrying this to the grant folks, push to get it in. And certainly in December we'll hope to hear what result of that was, what exactly -- what was done and exactly what the result was with Privacy Office efforts. So, thanks, Joanne.

MR. BEALES: Anyone else? Is there a motion to approve the report?

UNKNOWN MALE: So moved.

UNKNOWN MALE: Is there a second?

MS. SOTTO: Second.

MR. BEALES: All in favor please say aye.

MEMBERS: Aye.

MR. BEALES: Any opposed? The report is adopted.

MS. SOTTO: Thank you.

MR. BEALES: All right. The Data Integrity and Information Protection Subcommittee. Ramon.

MR. BARQUIN: Thank you. We have been tasked and are happy to have accepted a task on what I think Hugo referred to in his comments as helping the [inaudible] with a scalable, reusable privacy model for service-oriented architecture for SOA, and we are just working with the Privacy Office to define specifically what the output from that tasking is going to be.

MR. BEALES: All right. Thank you. And the Subcommittee on Data Acquisition and Use. Richard.

MR. PURCELL: Thank you. We continue to work on tasking on developing guidelines around the Memorandum of Understanding and computer matching agreements for information sharing. We were briefed by the Office of Inspector General for the Department in July and we are building out a framework upon which we can base the guidance that we are developing now. We hope to work closely with Toby in the Privacy Office, continue working with -- under her leadership to provide this by the December meeting.

MR. BEALES: All right. And thank you very much. Just so that it's -- as a matter of the record, I guess, of the Advisory Committee, we've also been tasked with looking at E-verify. I think the most efficient way for us to do that is through a separate subcommittee and we will be in the next couple of days designating people for that separate subcommittee. I would really like volunteers, but I guess I also consider myself a draft board if necessary. So -- Neville?

MR. PATTINSON: [Speaking off microphone].

MR. BEALES: Thank you very much. Thank you. I mean, it doesn't have to be right this minute. That wasn't what I was asking, but the -- I would like volunteers to -- so that we can make that. And I wanted it to be on the record of this meeting that this is a subcommittee that's going to be doing work as well.

All right. We have gotten to the important item of the agenda, and that's lunch. And so we will take a break for lunch and our administrative session. Please be sure

you're back. We will start promptly at 1:00 because many people have planes at the end of the day and we would like to get as much done before they have to leave as we possibly can. And if you are interested in making a public comment, please sign up at the table just outside the door.

Thank you. And we will see you at 1:00.

END OF MORNING SESSION.

AFTERNOON SESSION:

MR. BEALES: We're going to begin with another panel of DHS Component Privacy Officers. And we will start with Paul Hasson, who is the acting Privacy Officer for US-VISIT. He joined the US-VISIT program in 2005, and before that he served as a Management and Program Analyst in US-VISIT's Business Policy and Planning branch and he developed the business requirements for some of the major program milestones. Mr. Hasson has just over 16 years of experience in border management and immigration issues and came to US-VISIT from Customs and Border Protection. He spent 13 years at L.A. airport, most recently as the Chief in Passenger Operations. He received a B.S. in Criminal Justice Administration from San Diego State University. Mr. Hasson, welcome, and we look forward to hearing from you.

And I guess what we'd like to do is go through -- we'll go one at a time and then come back to questions at the end.

MR. HASSON: Okay. Can you hear me? Press this down. It's working?

MR. BEALES: It is working, but unfortunately you have to hold it down.

MR. HASSON: Okay. I'm holding it. Thank you very much for introducing me and the opportunity to speak to the Committee today. It's my first chance, so especially I appreciate the introduction.

I know, as Hugo mentioned earlier, we've had a Privacy Officer ever since we stood up at US-VISIT five years ago, and I know that you all have had the opportunity to hear from various folks from US-VISIT over the last few years. So I'll be brief. [Inaudible] give a little bit of introduction to US-VISIT since I'm sure you're all quite familiar.

I do know that US-VISIT appreciates the expertise and perspective that this Committee brings to the Department, and I look forward to continuing the tradition of communication with you all.

Just a real quick background for those who are not familiar with US-VISIT; I'll make it really brief. We provide the biometric identification analysis services to various federal, state, and local agencies -- government agencies. Associated most with US-

VISIT are the biometrics, meaning the fingerprints and photographs as well from international passengers at U.S. visa issuing posts and at ports of entry.

Across government, US-VISIT is helping prevent the use of fraudulent documents, protect visitors from identify theft, and stop thousands of criminals and immigration violators from entering the country.

We understand that our program's success relies largely on our ability to not only maintain the integrity of the information we collect but also ensure that it is protected from misuse both within and outside the government. That's why US-VISIT has always taken a comprehensive approach to protecting visitors' privacy.

As someone who has been actively involved in the planning and execution of US-VISIT's initiatives, I can tell you privacy considerations truly are built into everything we do from conception to execution. Responsible stewardship is a job we take very seriously at US-VISIT and it's fundamental to how we do business. I'd like to provide you with three examples of how we bring this to light. First, we not only hold ourselves to our privacy principles but we hold our partners to these principles as well. We make sure that any government agency that has access to that information is fully trained in our privacy practices and we have clear and comprehensive parameters in place that govern how they can use this information. Second, we publish Privacy Impact Assessments for each new initiative we undertake. Our PIA's have been publicly recognized as models for providing a transparent view of what information we collect, how we store it, and our policies and practices to ensure the information is not abused. Third, we protect our data systems. US-VISIT systems are carefully monitored and we have security practices in place to protect the privacy of those whose data we collect and to ensure the integrity of that data.

Of course what really matters is not just what our principles are but how we apply all of them to our program activities. So now I want to update you on two of our perhaps most important initiatives going on right now at US-VISIT that transition from two to ten fingerprint capture or collection and the deployment of biometric exit procedures to the different environments -- air, sea, and land.

As you know, US-VISIT is in the process of transitioning from a two-fingerprint collection standard to one based on ten fingerprints. Some people ask, ''Why collect more fingerprints?'' By collecting more fingerprints we have more information against which to verify an international visitor's identity. This makes the process faster and more accurate; it also reduces the possibility that our system will misidentify an international visitor. While this doesn't happen often, reducing mismatches makes travel more efficient for legitimate visitors and enables us to focus our attention on those who pose a risk to the United States.

When we began in 2004, the technology that was required to collect ten fingerprints just didn't exist. So the program began based on a two-fingerprint standard while we worked with industry to develop the necessary ten-fingerprint technology. Ten-

fingerprint scanners have since been deployed to all State Department visa issuing posts; and currently we're at 11 ports of entry here in the U.S. The deployment has been successful so far and we will continue upgrading to the ten-fingerprint scanners at all U.S. ports of entry this year and plan to complete deployment to all U.S. ports of entry next year in 2009.

Another of US-VISIT's priorities with which I'm sure you're familiar is the deployment of biometric exit procedures. Our first priority is deploying biometric exit procedures to airports and seaports. This past April, April 24th, we published a proposed rule in the Federal Register that would require those non-U.S. citizens who currently provide biometrics upon entering the United States to also provide digital fingerprints before leaving the United States by air or sea. The proposed rule would require commercial air carriers and cruise line owners and operators to collect and transmit international visitors' biometric information to DHS within 24 hours of leaving the United States by plane or vessel. The proposed rule does give carriers latitude to determine where in the airport or the seaport facility they would be able to collect the biometrics.

To protect the privacy of international visitors, DHS would require that those collection systems meet DHS' transmission standards and data security -- excuse me -- transmission and data security standards. The proposed rule also states that carriers can only use the biometrics they collect for the purposes of transmitting a biometric departure manifest to US-VISIT. Carriers will be prohibited from using the biometric data for any other purpose.

We received more than a hundred comments on this proposal, and taking these comments under consideration we are now working to publish a final rule outlining new requirements and the data on which they will take effect. We anticipate deploying procedures at airports and seaports in 2009.

At the same time we've done [inaudible] solutions for the air and sea environment, US-VISIT has also [inaudible] solutions for biometric exit procedures in the land border environment. People depart the U.S. through land border ports in a variety of ways, of course, that I'm sure you all know -- by foot, by car, bicycle, all sorts of manners. And there is no one solution that would be the one-size fits all.

US-VISIT sought out the best thinking on this. In June we published a request for information and held an industry day briefing to ask industry for information and recommendations. We need to know what is possible today, more specifically, what can we do right now and can we do it with commercial off-the-shelf technology.

Well, what's in the short to medium term pipeline? What may not be possible today but will be possible in the next, say, three to five years? Third, what's in the still in development technology pipeline that will take more than the five year period? In what timeframe might those future innovations be available?

And finally, what simply can't be done with known technology? What are the limits of technology? What can't we do and why not? Industry [inaudible] response of key component in US-VISIT's preparation for a report due to the Secretary -- to Secretary Chertoff that will inform the next steps on land/border exit procedures as well as any future acquisition process.

Once a land border solution is agreed upon, we expect to deploy in phases that will address the different modes of transportation as I mentioned a moment ago, such as vehicles and pedestrians at our borders.

And of course, in keeping with US-VISIT's Guidant principles, whatever technology and processes the program moves forward with, you can be certain [audio cuts out] program will be focused not just on enhancing security but on facilitating legitimate travel and trade, and of course, protecting visitors' privacy as well.

With that, I conclude my prepared remarks and once the panel is done I'll be happy to answer any questions you all might have.

MR. BEALES: All right. Thank you very much. Our next panelist is Pamela Carcirieri, who is the Deputy Director for Privacy at the Federal Emergency Management Agency. I imagine it's been busy lately. She served as Deputy Director since October of 2007. Before that she was the Departmental Privacy Officer, Departmental Records Administration at the Department of Transportation. Ms. Carcirieri has 27 years of government service, most of her career working for the Army at Aberdeen Proving Grounds in Maryland, and then at Fort Belvoir in Virginia. She's a graduate of the Modern Archives Institute and has completed numerous development and certification programs through the Army. Welcome. We look forward to hearing from you.

MS. CARCIRIERI: Hi. Can you hear me? Is this okay? Thank you very much. I am Pam Carcirieri; I'm the Deputy Director for Privacy at FEMA, and I'm speaking today on behalf of John Sullivan who is the appointed FEMA Privacy Officer.

And I just want to echo my colleagues and say that it is my honor and my privilege to be here today and speak to you.

First, I thought I would talk a little bit about what FEMA does. FEMA coordinates the Federal Government's role in preparing for, preventing, responding to, and recovering from all domestic disasters whether natural or manmade. A natural -- hurricanes, wildfires, et cetera. Man made -- 9/11. FEMA can actually -- what I think is interesting -- can trace its beginnings way back to The Congressional Act of 1803. This Act is generally considered the first piece of disaster legislation, and provided assistance to a New Hampshire town following an extensive fire.

So if we jump forward to 1979, President Carter issued Executive Order 12127, and that merged many of the separate disaster related ad hoc responsibilities into one agency, which is the Federal Emergency Management Agency.

The new FEMA was also faced with a lot of unusual challenges, such as the contamination of the Love Canal, the Cuban Refugee Crisis, and the accident at Three Mile Island.

So I have handouts for all of you, and if you look on Slide 2, you can see how the Privacy Office is structured at FEMA. I fall under the Records Management Division, and our Division is comprised of four branches and offices addressing records management, directives, forms, privacy, FOIA, and collections which cover the Paperwork Reduction Act. We currently have about 45 individuals in the entire division.

Slide 3 provides the organizational structure of the Privacy Office. As I stated earlier, Mr. Sullivan is the appointed FEMA Privacy Officer and I serve as his designate. I am so fortunate that I was able to obtain the additional help in the four individuals listed on this slide, and they have all began working with me recently.

So some of you here might actually know more about the privacy program at FEMA than I do -- the background. But, on Slide 4, you can see the Privacy Program was pretty much un-resourced until October 28th, 2007, which coincidentally, is when I started. And when I walked through the door, the FISMA score for FEMA was PIA's and SORN was at 8 percent for PIA's and 48 percent for SORN's.

So I'd like to just talk about some of the positive things that my group has accomplished since that time. We've been able to prepare and submit a memorandum to Administrator Paulison to increase awareness, further protecting PII and highlighting that. We've been able to substantially reduce the collection of Social Security Numbers on all of FEMA forms. And in less than a year we've been able to almost double both the PIA and SORN scores as well as complete several of the Legacy SORN actions.

And near and dear to my heart is -- and just this month we've been able to launch a FEMA privacy website on our intranet.

So continuing on Slide 6, we also have a very active training program. As we've reported it to DHS in our 803 reports, we have held approximately 62 briefings with over 1,300 people in attendance. And FEMA is very fortunate that we have several people in our Office of Chief Counsel as well as our security division that care just as much about privacy as we all do and that training indicates the briefings that they conduct as well.

We've streamlined the PII incident reporting process and something as simple as creating an email address with all the correct people and distribution has really increased efficiency as far as responding to a breach.

And finally, we've been able to update a 1987 privacy directive.

So I know some people have more robust privacy programs, and we are still very much a fledgling agency program in the making. But I think it indicates forward progress, and that's a good thing.

Some of the challenges we face - of course, the FISMA score is going to remain one of our biggest priorities. But I also think rogue systems; we have a lot of IT systems that I think that are unaccounted for and that are under our radar screen. I think that poses a problem. And I'd like to see privacy awareness as far as web-based training; I think that would be a good thing. Resources are going to remain a constant struggle, both people and dollars.

And the last bullet that I have about the hurricanes, wildfires, and earthquakes and floods, that's a real challenge since responding to these types of disasters is FEMA's business. And that means that when an event like Hurricane Ike occurs, the subject matter expert that I was working with on a particular or PII or SORN is now called away to assist with emergency operations.

So that's pretty much what I have. And I'll turn it over to my colleague.

MR. BEALES: All right. Thank you very much. Our third speaker is David Roberts from the U.S. Coast Guard. He joined the Headquarters' Privacy staff in June of this year. He recently retired from active military duty with the Coast Guard as Lieutenant Commander after over 29 years of service -- looks like his best assignment was Honolulu. In 2007, he received a Bachelor of Arts degree in Liberal Studies from Excelsior College in Albany, New York; and he currently lives in Fairfax. Welcome, Mr. Roberts.

MR. ROBERTS: Thank you very much. As indicated, I've been with the Coast Guard for quite awhile but I am new to privacy, so I am very thankful to have the opportunity to remain with the Coast Guard and the DHS team.

I wanted to briefly give a Coast Guard overview and then talk about some of the responsibilities and roles that we have in the Privacy Office. The Coast Guard is a multi-mission organization. The primary roles are Maritime security, safety, protection of natural resources, Maritime mobility, and national defense. Within those roles lie law enforcement, recreational boating safety, search and rescue, and a myriad of other responsibilities.

Our personnel resources include 41,000 active duty members. To put that number in perspective, the New York City Police Department has 39,000, so we're barely larger than the New York City Police Department. When you add the civilians and the reservists to that number we grow to about 57,000. And to put that number in perspective with where we are today, there are about -- over 125,000 rooms in Las Vegas. If all the Coast Guard was here on the same day we wouldn't even fill half those rooms. So the Coast Guard is a big player in DHS, but as an armed force, we're very small. And I just wanted to share that with you.

The Coast Guard Privacy Office is located at Headquarters in Washington, DC, and for those of you familiar with DC, it's the old FBI Building on Half Street in Southwest. We're part of the Command, Control, Communications, Computers, and Information Technology Directorate, which is commonly referred to as C4IT. Rear Admiral Glenn is the Assistant Commandant for C4IT, and he's also the Chief Information Officer. Below him in the privacy chain is Sherry Richards, and she is the Chief of the Office of Information Management. And then next in line is Yvonne Coates and she's the Chief Management Programs and Policy Division. As you work your way down that organizational chain, privacy falls with FOIA, Records Management, mail, e-Government, forms management; we sit there with those, and there are only two people that are dedicated full-time to privacy. So that number of 57,000 people where there are only two of us doing it full-time that certainly is an issue. And although I've only been there a brief time, I see the under-staffed as being a -- certainly a big issue.

Primary duties and responsibilities: certainly, PTA's, PIA's, and SORN's, which, you know, we all deal with. We work with the programs to ensure compliance. We liaison with the DHS staff, so we're the go-between. We do not write PIA's and we never will; we just don't have the staff. But we certainly look at them, review them, pass them up -- they go back and forth with all the iterations.

We have 67 SORN's, we have 122 systems under those SORN's and, as you've heard from others, we are certainly re-issuing, combining, and retiring systems as we can. And, I mean, we have things that go back when we were still Department of Transportation, so that's a big undertaking but we are making progress.

I was also asked to briefly talk about how we handle incidents, which we certainly have some of those. And I ran some numbers, and the numbers have been increasing every year -- the number of incidents we have -- but I think that's kind of a good thing in that there's awareness, people understand what they have to report. But certainly, I would say when we get done and start talking about training, the teaching people the safeguarding to prevent incidents in certainly paramount as the next step. So awareness is one thing, it gets those reports out, but safeguarding it is the next step. So as far as incidents go, we have an outlying unit will report an incident to the Coast Guard CIRT, which stands for the Computer Incident Response Team, and they're located in Alexandria, Virginia. Those folks then report to us; the 611 staff at headquarters. As soon as we get that, we reach out to the unit, we'll talk to the point of contact, we'll gather additional information, we'll fill in the gaps that the report might not have on it to make sure that we understand exactly what transpired. We'll tell the unit exactly what they're going to be responsible to do in order to close this particular incident. We advise them to seek legal counsel, we talk to them about mitigation and remediation, the training that's going to be required, depending on the severity of the incident, as to what the steps that's going to have to happen.

Next, we inform CIRT to go ahead and report that up to DHS-SOC so that it becomes a formal incident, it's in the system for all to see and monitor, daily reports are required when it involves PII.

And then lastly, we report to CGCIRT to advise DHS-SOC when to recommend to close that incident, but we never do that until all the requirements have been met. We make sure that if someone is supposed to get credit monitoring, that in fact has been offered, and either accepted or declined. So we make sure that everything that's suppose to happen, happen before we recommend closure.

One of the other responsibilities we have -- our directives review. The Coast Guard puts out a lot of instructions, a lot of manuals, a lot of messages, notices, publications; and we in the Privacy Office have to review every one of those with our privacy eyes to make sure that those documents are in compliance. And so that takes a significant amount of time. The instructions could be something as brief as two or three pages or it could be a manual that's 250 pages, and we have to look at that to make sure that if they're talking about PII or their system or whatever it is to make sure that it's in compliance. And that is a heavy lift for us.

In addition to reviewing the documents and directives that are generated through all the directorates, we also need to establish our own policy for privacy. And as OMB or DHS pushes that stuff down, we take that and then generate our own instructions to make sure that the outlying units understand what their role is. And that's a difficult one for us. Our FOIA and Privacy Act manual that the Coast Guard owns is a bit outdated and needs some work, and with all of our other responsibilities, it's difficult to get that thing rewritten so that it's current and up to date. But it does need to happen, so not only are we looking at everyone else's work, we need to do our own work as well.

And with that, certainly, we draft messages to tell the field what the current issues are in privacy to keep them up to date and informed.

I say that there are only two people that work privacy full-time, but certainly, we have people that do it on a part-time as a collateral duty in the field. And it's -- with the training and the instructions and websites that we provide information to keep them up to speed.

Lastly, there is a training element which this past April before I was there they had a very successful Privacy Awareness Week. And what they did was throughout the week each day they would have different presentations, we would visit with different systems owners to educate them, there were posters, there were opportunities to engage with the Privacy staff. And we had full support from all the directives, and so formalizing a training I don't item like that was a week long, we got a lot of visibility and it was very successful. And we will certainly be doing that on an annual basis.

Additionally, we publish articles in Coast Guard publications to, again, get the privacy word out. In training, like I said before, certainly an integral part in reducing

incidents and it's the safeguarding versus the awareness that I see as our next step with the Coast Guard.

As far as goals go, it's the undermanned staff that we have. I think in order to be truly effective and to address all the issues that we have facing us, we need to get enough people in there in order to effectively run this program. Daily, it seems like its crisis management because so many things come up and we just -- there's just the two of us. So I see that as a big step for us, is -- and we do have resource proposals in place and there is a -- will be an opportunity to add staff to -- additional staff numbers. So, thank you.

MR. BEALES: All right. I want to thank all three of you for being with us today. Neville Pattinson.

MR. PATTINSON: Thank you, Howard. Thank you, Panel, very interesting presentation of information. I have a question for -- on the US-VISIT system. We have an increasing number of countries issuing electronic passports to their citizens, and as they come to this country, are you equipped adequately with possible readers? And is the electronic passport helping the US-VISIT program capture data accurately or organize it? Is it affecting the speed of the transaction? Is it too early to tell?

MR. HASSON: Thank you. Operationally, when I was on the Business and Planning -- well, I was actually on the Business Planning team -- Business Requirement, so I was part of the team, sending them out to the field and having the opportunity to see them first hand -- they were working well. And don't get me wrong, I didn't mean [inaudible] meaning when I was out there, I observed it personally, and from what I understand they still are. That's probably a better question from -- for CBP and the operations side of CBP to make a determination. As a former manager in the field for CBP, one of the true signs of how effective or efficient it is if it's holding up the line. But from what I -- the reports I've had back is the timing -- the extra time wasn't significant, actually, during the course of the inspection. So, so far from what I understand, it's been operationally a successful deployment.

MR. BEALES: Joanne McNabb.

MS. MCNABB: I was interested, Panel, in your SSN reduction program, something I think a lot of organizations are working on right now. And what sort of things did you discover when you started looking for uses that you were able to eliminate?

MS. CARCIRIERI: Thank you. What they did was, and this actually happened before I came on board, they had reviewed all the forms that came. What works well at FEMA is the fact that Records Management and Forms is with Privacy. So that creates an opportunity there. I believe what they found was that the Social Security Number was actually being collected unnecessarily, and it was a practice previous to always routinely

collect something. And then going back to that proponent and seeing if they actually need it. So --

MS. MCNABB: And how did you deal with the, I've found, often daunting task of driving the old forms out of circulation with new forms?

MS. CARCIRIERI: Well, and that's exactly what we did was make them obsolete and remove them from our electronic share drive, so then they weren't accessible any longer.

MS. MCNABB: But they're still out there, you can bet.

MR. BEALES: John Sabo.

MS. SABO: Two questions, one for Paul and then the rest for the panel. First question -- if I understood it right in the [inaudible], did you say that in the ten-print system that biometric data elements are being sent to the airlines, or did I miss understand that? I think -- I made notes -- airline systems and there's a policy agreement they need to sign. Or am I mixing that up with something?

MR. HASSON: Those were on the -- I think there may have been confusion. I spoke of two different programs we're in the process of implementing and developing. One was the ten-print transition, and that goes to IDENT, to the US-VISIT system just as the two-prints do; it doesn't go to the airlines.

MR. SABO: All right. Sorry for -- the broader question for everybody is, as a group of Privacy Officers or people working for Privacy Officers, do you on any kind of regular basis convene Privacy Officer forums where you talk about these collective issues of, you know, like, Joe had mentioned earlier in one of the prior panels about the architecture of privacy and how all of our systems are interconnected, but do you on any kind of basis get together as a collective group of officers to share practices or look at issues that you should tackle together, that kind of thing?

MR. HASSON: I can start out. From a lessons learned or an issues point-of-view, we do have the opportunity to meet, and both of us know each other. The DHS Privacy Office holds monthly meetings so we do have an open forum and we are able to discuss outstanding issues with each other and compliance and perhaps lessons learned.

As far as the architecture from a technical side, at least with us, it's more internal. We meet with our internal stakeholders on how to work that out.

MR. ROBERTS: And I'd like to add, from yesterday's get together I learned that they do -- we do have task force groups that get together on a particular item and work something to resolution. So depending on the item and the subject matter, there are opportunities to work with each other with DHS to resolve issues. So --

MR. BEALES: All right. Are there any other questions? Okay. Well, thank you very much for being with us. We appreciate your presentations.

Next item on our agenda is preserving privacy and research on physical screening. And with us today we have Dr. Susan Hallowell, who is the Director of the Transportation Security Laboratory of the Science and Technology Directorate of the Department of Homeland Security, or as she described it to me earlier in a conversation, her office builds bombs and then tries to find them.

The laboratory is responsible for researching, developing, and evaluating solutions to detect, deter, and mitigate improvised explosive devices. Before this position, she was manager of the Explosives and Weapons Detection R&D Branch of the Transportation Security Laboratory. She's worked for DHS, TSA, and FAA for over 15 years in the area of explosives detection research and development and is an expert in the area of trace detection of explosives. Prior to working for the FAA, she worked as a research chemist for the U.S. Army, and again, in detection and protection against chemical warfare agents and technical measures supporting chemical warfare treaty verification. She was granted a PhD in analytical chemistry from the University of Delaware in 1989 for work on biosensor development. She holds a Bachelor of Arts from Western Maryland College with a major in Chemistry. Dr. Hallowell, welcome. We look forward to your presentation.

DR. HALLOWELL: Thank you so much, Mr. Beales. It's a pleasure to be here. Let me see if I can get this going for us.

UNKNOWN: [Speaking off microphone].

DR. HALLOWELL: Oh, while we're getting started -- I'm going to go ahead and start and we can catch the [audio cuts out].

MR. BEALES: Sadly, you have to either hold the button down or weight the button down for the microphone to keep working.

DR. HALLOWELL: The computer would work. I think I'm just going to press the button.

The TSL is an element of the Science and Technology Directorate, and we are actually a federal laboratory with the core mission of developing technologies to find explosives or mitigate against explosives, principally in the transportation security sector, although our mission is evolving. My laboratory used to be an element of the Transportation Security Administration; we no longer are. We are a service provider to TSA as a customer. We are an R&D laboratory that also does tests and evaluation, and again, our mission is to research, development, test, and evaluation on emerging technologies that may have some relevancy for homeland security protection. Having said that, we mostly work in the area of IED detection.

I'm not going to go through this whole presentation because I don't believe I will have the time, so I will give a little bit of background on the laboratory and [inaudible] I can show a very fast video which is sort of interesting. I'm going to skip the relevant legal guidance policy, although I will just say that I have spent some time trying to understand what kind of legal guidance I could get from some court rulings relevant to Fourth Amendment Rights as it is relative to physical screening.

I will talk a little bit about the scientific approaches we have developed to provide our customer, which has principally been TSA, various security options when they go to security deployment. A little bit about our test the evaluation and a little bit about some of the guidance that we offer our customers.

I sort of went through this; I think the relevant thing off the slide is that we're located in Atlantic City, New Jersey. We have actually been there for a number of years. The genesis of my laboratory is the Pan Am 103/Lockerbie incident, which of course, all [inaudible] were lost was because a improvised explosive device had been sequestered into checked baggage. That was the start of the laboratory; it resulted in our laboratory being built and we were off and running. At that point, we were an element of the Federal Aviation Administration.

We think about how explosives can be introduced into the transportation security system in terms of the threat vector, and we've designed our programs around protecting these different threat vectors into an airport onto an airplane. We put together didactic teams of scientists, engineers, and human factors, explosive handlers, and anybody else we need to produce a product lines in research and development that are suitable for [inaudible] by our customer.

What I think I will do at this point is quickly try to show you a video of the laboratory, only because it says so much more than I could probably PowerPoint through. Oops. That did not work.

[Video begins]

Okay. This is a typical morning at the TSL. This is one of our explosive handlers that's going to a bunker that contains explosives and explosive built and test articles that are mostly checked baggage. Again, what we attempt to do is to -- by utilizing both intel sources and our own cleverness, build improvised explosive devices that we think are representative of the current threat.

This is actually our bomb-making factory. You'll notice there's toys, there's clocks, there's shoes; we have made everything into bombs.

This is one of our explosive handlers, Dave Hernandez [phonetic], who is about to put C4 into a toy. You're looking at the various components associated with improvised explosive device. There's the major charge. He also has a switching device, a detonator, and a battery to power this. Okay. Now he's placing it on carry-on baggage.

Okay. This is Lab 1. What you see is some prototypical devices that are not yet certified that are designed for interrogation of carry-on baggage. It's computer-aided tomography, which is technology which we shamelessly stole from medical community, and applied it for homeland security applications. And what you're looking at is a cross-sectional image which you can rotate in 3D of the bag. Now, if you note, the -- this red area is actually the C4 that has been picked out. It's actually quite clever. The detection is based upon the average Z-value of the explosives; therefore, you can pick up explosives in a sea of interference. Not perfect. There are some false alarms occasionally; we all know that because we travel in airports. I'm not liking the way he disappeared. Here we go.

The next thing we're going to look at is the fabrication of a suicide vest. We're looking at three sticks of dynamites and some connections and some switching items. This is something that we've been working very hard on with TSA for the last 18 months or so in terms of evaluating whole body imagers designed for imaging suicide vests or other weapons of mass destruction that have been clandestinely concealed on people. This is Theresa McGee, she is our lady explosive handler device who will be modeling our vest today. And as you can see, you really can't see it. Now, this is a trace puffer portal. This is something that also came out of our R&D program. We have her walk through it. The way this works is it looks for trace explosive residue. It turns out Theresa was hotter than a firecracker this day. The devices are actually exquisitely sensitive for explosives and highly specific. She's not being allowed; she's getting the red hand. So she would be pulled out of line. There is no earthly reason why you should have C4 on you. Once in awhile we do find people that are traveling that blow up avalanches for a living and they may actually have a legitimate reason for having C4 on them. Occasionally I have C4 on me when I travel, but I've been out at laboratory, so --

Okay. This next video here is actually a whole body imager that's using a radar detection technology. Again, the suicide vest showed up quite well.

Detection of weapons -- this is one of our bright young scientists who we asked to be a volunteer, who actually has a few weapons concealed on him. He was a good candidate for the show because he's very, very skinny and he has many weapons on him. Again, this is millimeter wave technology and you can see the number of weapons he has on him. Note that in this particular clip, the face has been shrouded with a cloud to prevent privacy. This is x-ray backscatter with a new privacy algorithm that we've incorporated into the technology as a result of our R&D effort. Notice the position he takes. We also evaluate different positions for security efficacy.

And as you can see, he has quite a few weapons on him. So what does Luther have on him? Well, he has a vest; he has a few guns, a few other guns. Oh, how did we forget that one? I'm going to cut this clip right now. We do a lot of research but that's not relevant to this, so I need to escape. Thank you. Or I can do it this way.

[Video ends]

So, I'm going to skip over the legal aspects of the guidance we have. This was actually a very interesting ruling by the Supreme Court. It came out June 11th, 2001, that was relevant to interdiction of illicit substances, meaning drugs, by using an IR camera. An important thing about this particular case was it sort of started drawing the lines as to what was permissible in terms of search and not search. Again, this was not detection of explosives, but the interesting thing about this case is that exactly three months later were the attacks of 9/11, and of course, the World Trade Center and the Pentagon were attacked. And this really was a game changer, and [inaudible] was immediately immobilized to design and deploy systems and devices not in general public use capable of detecting CBRNE weapons.

Subsequent court decisions sort of elaborated on what this meant to us as technologists. The location of the search is quite important. Obviously, there is great expectation of privacy in somebody's private home and even in their car, but there is little or no expectation of privacy when you're outside the borders. The activity being revealed by the search, obviously we need to restrict that to detection of weapons and the material being searched and what technologies are being used.

I guess I was struck by the fact that early on in 2002, the courts had done some elaboration as to what privacy was but it really hadn't come home to the R&D community, those who were responsible for building the technology. And we had been doing that since -- Transportation Security Laboratory as a session of the Gordon Research Conference that I was in charge of a number of years ago -- I actually had a session on privacy and I brought together the ACLU, government officials, and also our industrial partners who are making the technology itself to have some discussions on what is appropriate.

In 2005, a very bright man named Don Prosnitz wrote a very good article on search and seizure of weapons of mass destruction, and certainly he make the point that we need to look at how we can incorporate technology during the R&D phase and not slap it on as an aftermath, after technology is fully developed. So, obviously, this is a balancing act. There's a tradeoff between security, safety, privacy, and customer service, and the trick is to get the tipping point just right.

So the question is, is it a reasonable search, and is the technology reasonable? And in order to do that we have to start translating privacy requirements into technical requirements from the standpoint of the technologists. And in order to do that we have to start examining receiver operating curves for technologies, and examine the technology itself and make decisions as to whether or not it's doing what it needs to do.

Obviously, the amount of time involved in interrogation is important. Those of you who travel through airports understand the time factor and certainly the degree of intrusiveness, which is not something that you can turn so much into a technical requirement. It does require opinions.

Now, how often can a sensor miss or declare the presence of an IED or other contraband? This is actually -- can be described by the receiver operating characteristic curves which are actually boring but very relevant to this discussion because it's how you tune an instrument in terms of sensitivity, and [inaudible] activity and privacy settings would certainly indicate that you want a very, very low level of false positives. You want to find all of the bombs, not most of the bombs.

How our security concerns would indicate that you have to have a very low level of false negatives. That is if I don't have explosives on me, make sure that I don't alarm the system and have to go to some kind of secondary more evasive [inaudible]. So the trick is to find the technology that has both a very low false positive and a low false negative rate.

This is a receiver operating characteristic curve from the medical community. My husband is a physician; he's a radiologist. This is for prostate cancer using nuclear magnetic resins, which doctors call magnetic resonance imaging. The point is there -- you can operate up and down this curve and perhaps I could -- I can't use a pointer here -- there is a tradeoff between the two positive fraction and the false positive fraction. So in order to get all of the cancer using this particular technology, you incur a very large false positive fraction. This is not unusually good receiver operating curve. This is something from my laboratory for a similar technology called nuclear quadrupole resonance, which is sort of like MRI with no magnet. If you look at the red curve, this is a very, very good receiver operating curve because you can see the probable detection is very, very high, and the probable false alarm is diminishingly low. This is a good technology. This is the kind of thing that you want to look at for finding a bomb.

So we can basically translate some of these privacy considerations into ten rules for people doing R&D. First off, consider the kind of technology you may want to use at the initiation of the technology development program. Try to identify technologies that by their very nature are highly sensitive and selective to the threat but are not inherently invasive to privacy. And when I say that, in the context of this, they will find a weapon of mass destruction but they will not necessarily tell if for instance you were undergoing radiation or chemotherapy. That is nobody's business. [Inaudible] is the greatest thing possible, had a very low false alarm for privacy but a very high probability of detection for security.

Point number four let machine vision determine the presence of contraband to the greatest extent possible. What is machine vision? Machine vision is how a catscanner actually finds the bomb when used as a explosive detection system, which is what we use in American airports right now. Machine vision is an automated algorithm that can automatically determine density or abz-value of the substance and match it to a wide variety of explosives and allows the correct detection explosives [inaudible] sea of interference. Does not require a human operator to make the find.

Now, we do know, of course -- and you know this -- that occasionally people do resolve alarms by human operators looking at the threat. The trick again is to keep that

diminishingly low. From the perspective of TSA, that's a good thing because it means if you have a very high probable detection but there's not a lot of false alarms, you can have less screeners and the throughput is greater.

Number five. If an alarm resolution is necessary, if possible, use a second automated process -- another machine to resolve the alarm.

Number six. If an operator needs to resolve an alarm, limit the search of the area to suspicious item only.

Number seven. Develop and evaluate a menu of security options for the customer that can be used and is adaptive to level of security. So the dermal threat goes up, you may want to go to another security setting on that device. If you have some intel information that a particular area or particular flight may be at risk, you may want to set up, watch up the dial and make a security higher priority.

Number eight. Explore the operational aspects of how the technology can be used by optimizing privacy during the test and evaluation and the operational phases, usually at the operational sites.

Verify the privacy options are in place prior to piloting. That's actually a configuration management issue to the industrial partner.

And finally, work with the customer to suggest ways of using security that will optimize privacy.

I'm not going to spend too much time on enabling technologies, but I think it's somewhat important to understand what the technologies are and how they relate to privacy. Trace detection of technology is utilized -- it is the art of finding a bomb by doing a chemical analysis on the surface or even on a parcel, looking for explosive residue. It turns out, if you fabricate a bomb, you always leave a trailing residue behind. And the current state of art equipment that we're currently using is so sensitive that it can readily find this bomb. We have deployed -- at least TSA has -- over 9,000 trace detection units to American airports and they're very successful in doing that. They're successful from a privacy concern in that they target explosive residue and a sea of interference, so you will find explosives but you will not find hand lotion, you will not find perfume, it will not alarm on other substances. Occasionally there are nuisance alarms. If you fertilize your front yard and then go to the airport, there is some possibility the nitrates will alarm the system. But from the standpoint of how this is being used, because of specificity, trace is a fairly good technology to use for explosives detection.

Now, you could do chemical analysis for other kinds of substances. And we don't do that. For instance, you could use chemical analysis in the far future to look at people's DNA. That's another privacy concern, but the reason why trace technology works is because of specificity of how a machine is set to see only bad things.

Moving on to bulk detection of explosives, that's sort of a euphemistic way of explaining if you have an explosive substance and you interact it with various parts of electromagnetic spectrum, you can create unique signals representative of explosives. We looked at various parts of this electromagnetic spectrum domain -- NQR -- nuclear quadrupole resonance -- is actually bombarding explosives with radio waves. That's actually quite specific. If you get a yes or no, it works with some explosives. It doesn't work for all explosives.

The radar rage is something that's been developed for whole-body imagers that are now being piloted at various American airports; that is an imaging technology.

There is another area which I don't think I put my cursor on -- yes. There is the terahertz range which we're looking at in R&D land which gives you some imaging and some chemical information. That's still very experimental. It seems to work in some cases; the technology is not quite there. There is some development that has to be done and then certainly the cost of detectors needs to go down.

Moving up to x-rays; I think we're all familiar with the x-ray backscatter technology. I happen to notice that it was in the USA Today. There was a portal that is being evaluated by TSA; that's x-ray backscatter that works by using very low energy x-rayers that actually reflect off of surfaces and give different information relevant to what the surface is. It does penetrate your clothing and you can certainly things clandestinely concealed on the body.

Human factors. The ultimate arbiter of an alarm ends up being a human. Use of the human and what they do with that information and how that information is stored is probably the trickiest part. That is pretty much procedural; the perspective is you want to get the humans involved in minimally; of course, they will have to resolve alarms.

So here's a partial list of what I just talked about. It's not totally inclusive because I notice that I left off computer-aided tomography. But there are some technologies that are inherently specific and selective that are very good from a privacy standpoint. There are other technologies that are very good for security that need privacy algorithms that we're currently developing or have been developed.

And I wanted to finish up by just going through a couple cases about how privacy is incorporated into some of the screening that has been done in American airports. This is an explosive detection system. These are in the basements of airports, sometimes in the front they are used to detect explosives inside checked baggage. Again, what you get is an image. What you also get, again, is this feature of an automated recognition of explosive; that's the red block that has been circled. A human will be called in only when this automated algorithm goes off and says there's something here that looks like explosives. It's within the window of an explosive compound.

This is a resolution image for explosive that was sequestered into a checked baggage. And you can very clearly see that the red line isn't [inaudible] good of [inaudible].

So from the standpoint of the privacy rules I just presented to you, there's very good receiver operating curves for EDS's and that they have high proper detections, low false alarm rates. Machine vision is used to alarm, and secondary alarm resolution is just in American airports by using choice explosive detection. Humans intervened to resolve alarms. They look at the picture on the screen and the look at certain features, such as, does it look like there's a detonator associated with wires and things like that.

Checkpoint is something that's emergent. We all know that checkpoint probably needs to have next degeneration technology apply for it; none of us wants to take off shoes. It needs to grow.

TSA has evaluated a number of technologies that we developed at the TSL with our industrial partners, and continues to enhance the checkpoint.

Explosive trace portals and whole body imaging technology have been technologies that TSA has piloted and utilized.

We have looked -- we have done research and development and test evaluation on metal detection -- the trace puffer portals, and finally, the whole body imaging technology which comes in two slightly different technological flavors, one is the backscatter imaging technology and the other one is the millimeter wave.

This is a depiction of the three different kinds of technologies. The one on the far left is the radar -- millimeter wave; the one in the middle is x-ray, back scatter technology; and the one on the right is trace.

I wanted to sort of skip through this slide. The important thing is that x-ray backscatter does penetrate articles of clothing and can see weapons and explosives quite well because of the contrast against the body. The problem with this technology is that it can be -- it produces a very disturbing image.

Whole body imaging assessment, here is -- I believe this is the millimeter wave technology. This is the millimeter wave technology. It produces a less-graphic, less-detailed image by virtue of the fact that the electromagnetic radiation has a much larger wave length. The image is sort of a speckled 19 holographic image that actually rotates, it helps the screeners make alarm resolutions by virtue of the motion of the image. In terms of our R&D, what we did to help this through is we had some major R&D programs that developed privacy algorithms and we evaluated the privacy algorithms as a function of both security, and that is still found the weapons and from a privacy standpoint -- and we performed a lot of test and evaluation in laboratory with mock passengers, evaluated different poses, and also assisted TSA in piloting these.

This is a very disturbing reference image. This is x-ray backscatter. You can obviously see why this is not acceptable and quite invasive for privacy concerns. We do not want to use these in American airports.

We developed a number edge algorithms that would show the edges of devices on people. We developed various algorithms that actually showed less and less resolution, that we presented to TSA and let them choose the privacy setting they felt was appropriate.

We did a fair lab assessment in the laboratory with mock passengers and created a lot of images that we could submit to federal security officers to evaluate performance of detection in the various privacy algorithms.

Just a note about our laboratory practices -- and I won't dwell on this -- we do have IRB, the governance of human subject protection. We've got an oral research [inaudible] through certified IRB's and we collect absolutely no information on our mock passengers. We don't know their names or anything at all.

Again, in terms of the state of the art right now, human interpretation is still essential but the [inaudible] images are not acceptable and we have developed a number of privacy algorithms. We understand there's a trade-off between privacy and security and we attempt to evaluate that. And we are currently focusing on research efforts on developing machine vision -- or [inaudible] detection algorithms for whole-body imaging. And we're focusing research on more material-specific detection.

And that really concludes my prepared remarks for the committee. If you have any questions. Thank you very much.

MR. BEALES: Thank you very much for being with us today. Are -- do we have questions?

MR. HOFFMAN: Dr. Hallowell, thank you for coming to speak with us. That was fascinating, actually. I would like, really, to commend you for the work that you're doing to integrate privacy into the research and development function. That's something that I know several of us in the high-tech sector have to do that ourselves over the course of a number of years, and I know that it's not easy work to get that done.

I actually would contend -- and I'd be interested in your comments on this -- but you're probably doing better than even your slides say that you're doing in that when I look at, especially the whole image scanner that you've got up there, it doesn't actually look to me like you are balancing privacy and security, which creates a presumption that go security you have to give up privacy. Instead, it looks to me as if you've got two variables which are privacy and security, and both of those become part of the problem that the engineers end up having to solve. Which I think is absolutely world-class; I think the research that's been done in this area by folks like Professor Latanya Sweeney at Carnegie Mellon have said, if you can position it not as a tradeoff but instead as two

values that are both problems that -- are aspects of the problem that have to be solved, so that the engineers can do what they're professionally trained to do, which is to solve those -- that problem with the two different factors, you end up getting something that is more secure and protective, potentially not just not decreasing privacy but increasing privacy. So I, once again, I would commend you and say I think you guys are doing better than even you're referencing in your slides.

DR. HALLOWELL: Well, thank you. Your description is actually much more elegant than mine. There probably is a tradeoff. I think most operators, if they had the opportunity, would go to a [inaudible] image and x-ray backscatter. But you're absolutely right; there is no underlying basis with that. You can probably work both issues as independent variables, yes.

MR. BEALES: I was curious about, you know, on your ten points, number four is, let machine vision determine whether there is a problem. And what we heard this morning from Jeff Jonas basically was really the advantages of letting the information -- the surveillance in the case he was talking about -- not trigger any automatic consequence but simply trigger human intervention. To some extent it's a different problem and I get in backscatter, you know, in the backscatter x-ray sort of approach, the advantage of letting a machine do everything as opposed to human intervention or combining -- confining human intervention for the very limited number of cases where you really need it. But it seems like in general there is some advantage of avoiding automatic consequences as a result of a decision that a machine makes as opposed to some human intervention. And I just wanted to get your thoughts on when and where is this the right rule as opposed to this is data, use it as human judgment tells you makes sense.

DR. HALLOWELL: Very interesting perspective. I'm going to hold on to the machine vision here because the technology, if it's extremely specific, just for an illicit substance that allows you to enrich the population you're going to search. I mean, you know, somebody comes through an airport and they have a bar of C4 on them and you have very good machine vision that means that only that person goes to a secondary kind of paradigm. If machine vision is good enough, that is certainly reasonable. A good analogy would be you go to your physician [inaudible] and he does blood work and he does x-rays; it's the same with aviation security. You do chemistry or you do some kind of imaging technology. And if you take the chemistry aspect, you're not flagged for additional examinations unless there is something that's really an outlier. The chemistry is very, very good. The chemistry is also very good for explosive detection, so think of it as a marker rather than -- probably not comparable to looking at behavior patterns or looking at suspicious behavior or other elements of surveillance that Mr. Jonas was talking about this morning.

MR. BEALES: Okay. Sort of the specificity of the test --

DR. HALLOWELL: Yes. Exactly correct.

MR. BEALES: -- if you will. Okay. Joe, we'll get to your question but we're going to have to pause to change the tape here.

MR. BEALES: Okay. Joe.

MR. JONAS: And thank you also for the presentation. But I wanted to follow up on Howard's question in a different light. And that light was when we met a lot of the agents who are at the border crossings and they were starting to talk about prepositioning of information and other types of things which were technological tools to help them, a concern arose that you want to make sure that as you're doing this, you don't take away the opportunity of the officer to observe types of behavior and that you don't want to create an overreliance on the tool. And so the questions becomes, the tools are very good at finding the guns, the knives, perhaps the C4, but maybe not Ricin or other things --

DR. HALLOWELL: Agreed.

MR. JONAS: -- that could be even much more problematic than those things, depending on the environment you're going into. And so I guess the question is, because the lab is so familiar with the tools, is there also practice guidance on placing the tools in context, or is that done by the agencies who use the tools, and do you work with them in understanding how not to -- or helping them not have an overreliance on the tool just because it's there?

DR. HALLOWELL: Very good point. The use of technologies is the slice of overall holistic approach to security. And TSA is our customer, but certainly Science and Technology Directorate is directly responsive to them because we build the R&D that produces things for them. And the whole area of suspicious behavior detection and [inaudible] and malicious intent is another layer that warrants R&D that is being examined within the R&D. The technology is really only good, there are some -- obviously some problems right now. The technology works really well at fixed checkpoints; will not work as well in places like train stations or other public venues. So the notion that we have to look at behavior or patterns of behavior is built into our security R&D program. It's not something I'm doing in my laboratory so much, but it's going to be a big element in the future and TSA has asked for that kind of research.

MR. JONAS: Maybe it needs to be done in a casino laboratory.

DR. HALLOWELL: Well, that's very funny because the last time I was at Las Vegas I was outed for suspicious behavior. And this big guy showed up and was blocking my exit from this place and I was rummaging in purse and I couldn't out. It turns out he was a security so I was outed for being suspicious and I was bad.

UNKNOWN MALE: Do we have any other questions? Alright, thank you very much for being with us.

DR. HALLOWELL: Thank you.

UNKNOWN MALE: This was a fascinating presentation.

DR. HALLOWELL: My pleasure.

MR. BEALES: Our final panel of the day will be an update from the DHS Science and Technology Directorate. With us, we have Dr. Jennifer O'Connor who is the Program Manager for Modeling and Simulation of the Human Factors Division. Maybe this is the behavioral laboratory. And she received her Ph.D. in 1997 from George Mason in Industrial Organizational Psychology, has served in a variety of R&D related positions in government, industry, and academia and on interagency working groups and subcommittees involved with research. Dr. O'Connor -- and -- okay. Is this one presentation or is this two?

UNKNOWN: [Speaking off microphone].

MR. BEALES: Two. Okay. Then I'll introduce you in a minute. To the audience, this is the last chance to sign up for public comments if you want; that would be at the end of this panel. If there are, at the table outside is the place to sign up.

DR. O'CONNOR: I wanted to say -- is it working?

MR. BEALES: Yeah. Unfortunately, you have to hold the button down to --

DR. O'CONNOR: Testing.

MR. BEALES: It's on. You're good.

DR. O'CONNOR: Okay. Thank you. Thank you very much for having me here today. I am from the Human Factors Division -- well --

MR. BEALES: We've electrocuted our guest.

DR. O'CONNOR: I may just have to press on like Jeff did. Okay. Okay. Thank you very much for having me here today. I am from the Human Factors -- recently, Human Factors changed to Human Factors Behavior Sciences Division, which is part of the Science and Technology Directorate. We are primarily a R&D function within S&T, and that's in -- actually, let me just back up for a second. It's R&D and transition funding. We are different from a lot of the other folks you heard earlier today in Privacy Office because we do this R&D function and some of our issues defer from the components R&D issues in the sense that when we first start doing our research we may need more personal information to get going, in order to [inaudible] down what actually is important, we're not using it for operational purposes at all. And consequently, there is fewer optional consequences at the beginning. And we have additional protections that they can't necessarily put in when you're using something more operationally. So that's

the general idea that I'm going to -- the point that I really want to make is that we are different than what you've heard previously because we are focused on R&D.

Our division has everything human. As it says in the title, it is Human Factors, so everything we do involves humans. We don't deal with law enforcement, we don't deal with intelligence, and we don't deal with operational determinations in terms of when we're doing our research. And we're different even from other components within S&T, like, explosives -- [inaudible] obviously does explosives at TSL, does transportation safety, et cetera.

We do quality research to try to make the homeland safer, to meet the highest scientific standards, and to make it timely and efficient. In other words, we want to do research that we can get out there and hopefully help to go operational as quickly as possible. But we're also trying to protect civil liberties, privacy concerns, and minimize the amount of PII that's used.

This is a basic flow of the types of research we do in terms of our focus areas. Analysis is just like it sounds. One of our primary programs in analysis is actually the one that I run, which is called VIMS, Violent Intent Modeling and Simulation, and it is intended to try to see what are indicators before they happen. I don't know if you guys have heard the term, ''we're trying to get left of the boom,'' to get as far left of the boom as possible by understanding when violence would come forth from a group and what would be triggers that would foretell that violence.

In the framework that VIMS works under, and this is kind of tricky with the Privacy Office, is primarily off of rhetoric otherwise known as open source press information. And to combine that with social science behavior, social science knowledge, social science theory, in a modeling and simulation -- couple of different modeling simulation frameworks, and be able to see if we could have predicted stuff earlier on.

And so you can see that there is -- one of the things that made it very complicated to explain and to have the Privacy Officer for S&T understand what was going on is that it wasn't -- we did not -- we -- there was a lot of theories out there in terms of when violence would erupt, but there was not a whole lot of empirical information backing it up; we're just now starting to get some of the data sets in that can provide this information. And consequently, we didn't really know as we got into it what types of PII we were going to need to actually predict these types of things because we were trying to do things at the aggregate level rather than at the individual PII level because we were looking at groups rather than people. And it gets into scientific methodology so it really became an education issue as well as -- on both parts, both on the part of the Privacy Office as well as on the part of the program managers to try to figure out where the happy medium was in terms of what really was the concern.

Moving on to the observation area, SPOT is one of our primary projects there and it's intended to see if you can look at behavior and get ahead of those that would do us harm in terms of deception, similar to what Mr. Paul Hasson was talking about earlier.

Interaction is the FAST program which built upon the observation of the SPOT program and adds into it physiological cues so that you can combine look and listen with non-invasive screen techniques like the weapons that Susan was talking about.

Then you get into the personal identification systems, and predicatively, they're biometrics, and that again gets into the ten-print technology that US-VISIT is interested in using.

Community preparedness and response gets into people issues where we're helping people recuperate. And, are you familiar with the 211 system that was in place during the hurricanes? It was a call-in line for help that victims of the hurricanes could use to try to get assistance either in housing or a whole range of things. And we're trying to do scientific studies off of that data to see what would have helped the most in terms of getting them up and running as quickly as possible.

Human systems research and engineering is watching how people interact with technology and making changes to it based upon the information that they have.

This kind of gives you an overview of our different frames of research that we have and the complexity of the requirements that are involved. To the -- if you go -- down first. This was an example of some of the drivers of the biometrics research where it talks about the Homeland Security Report, the one that just came out day before yesterday, or it was at least day before yesterday afternoon -- and has things in there specifically about the US-VISIT program. And then we have mandates from Congress, from international agreements, and these are some of our international circle exchanges -- some of our international partners as well as some of the other agencies that we're working with.

And then we have some issues from the operational components that drive our research in terms of what they want to see happen and when they want to see it happen. And international agreements, as I mentioned, multiple partnerships were working -- part of the VIMS research has been picked up by DOD and by the Department of Energy for looking specifically at some of the nuclear -- domestic nuclear issues. So we're working with them to try to take a piece of VIMS that has been successful and incorporate that into some of the other systems that they have.

We have legal requirements, obviously. And then the program down the slide looks at deter -- it starts with deter, predict, detect, respond, defeat -- is an example of where everything flows together. It's kind of a cascading effect so that it -- when we don't -- if we're not able to get our PIA's through the system, one project that doesn't get started on time could end up backing the entire set of projects up. So it wouldn't be just

one project that was slowed down in the process, it would actually end up being maybe three or four because they all tend to rely upon each other to get through.

Challenges -- I was asked to discuss some of the challenges that face program managers. Tight timelines, just like in Components, we're given operational -- especially when you have -- when it's an operational requirement or an operational need, they tend to come to us and say, you know, ''Can you guys do this?'' and we want to say yes because we're R&D and we want to save people and lives and protect the nation. But on the other hand, the reality sometimes is the research just isn't there yet. We get budgets; budgets are constantly changing. The continuing resolution being the latest case in point. You don't know how much money you're going to have and when you're going to have it by so you're constantly downsizing or upsizing your programs or trying to figure out what you can cut out, what you can't, how they mesh together. Meanwhile, the customers are -- as we call -- the other components within DHS, we consider them our customers -- may have requirements that change or their expectations may, you know, scope being what it is, may broaden out.

And then we have the people that are actually doing the research for us, our performers. We have to remind them constantly of privacy concerns and trying to keep them on track so that they're not getting ahead of themselves or getting ahead of what we're doing, and hopefully not talking too much to the customer because that tends to really cause problems. It's kind of a catch-22; you want them talking but you don't want them talking. Congressional mandates that we get periodically where we're told we need to do a specific kind of research. For instance, counter-id's is one area that we're working pretty heavily right now within the U.S.

The privacy itself has been a challenge just because I knew Mr. Teufel mentioned that he was -- that they had gotten down the privacy reviews to two-months time period. Unfortunately, for us on some of our budgets and some of our projects, two years might be a quarter or a third of the amount of time that we're given to do it in, and the amount of money that we have goes away if we don't get it done within that time period. So the further left we can push our understanding of what needs to be done for the privacy concerns, the better off we are so that we're not left sitting there. And this happened to me specifically with VIMS, we had to completely stop doing a part of the project because I was told by the Privacy Officers that we might be in violation of some of the privacy concerns. That's where Jennifer was incredibly helpful in terms of us trying to work through with everybody so that we weren't violating, and we were really trying not violating the civil rights or privacy concerns. But in the meantime, I was losing performers because they were getting -- because they were -- they'd stop work or -- so they were going off to do other projects and the money was -- they were telling me my money was going to go away and it was a five-year project so it was kind of -- the whole thing was kind of snowballed. It started rolling and we needed to find some way to melt it down pretty quickly. And I guess what I'm trying to say is, two months, really, for R&D anyway, some of the components that can deal with it because they're dealing with larger budgets and even more complex technologies. But for us in R&D, some of your R&D projects might only be six months because we're dealing with professors that are

doing most of the research during the summertime or industry that's used to doing the projects in, like, six weeks to two months and just getting them done. So waiting for a PIA to get through or for feedback from the Privacy Office is really important to this to make it happen as quickly as possible.

And then of course it's the nature of R&D, you might think you're going to go one direction with a topic, and get in there and find out once you get a little data that you're completely wrong and you've got to go a different direction. And with -- when you're studying people, that's probably not surprising to anybody; that happens fairly frequently. What you think is happening is not happening.

And I'm, for instance, doing a modeling project right now where we thought one of the predictors was going to, you know, we were looking at people's behavior and we were looking to see whether -- how buzz about movies spread and what they were saying, and hopefully predicting, you know, like the types of things people would be saying would indicate how successful a movie was going to be. And we had just kind of collected on the side -- or it was collected on the side just the amount of information that was exchanged -- turned out had nothing to do with what they were saying, it was just the amount of -- they were -- how much they were actually talking about it. So it was just by chance we had collected that extra information. And this is a perfect example of where it kind of gets confusing, if it -- in PII information, we could have been collecting non-PII information just a rote part of being consistent in your project and would have found out that we could have completely dumped the PII information and just used the other information to draw the conclusions, which would have been better for everybody. But, unfortunately, as I said a second ago, you don't know that until you get in there sometimes.

One of the things we had done to try to become proactive -- or, to be more proactive, is put together this Community Perspectives and Technology Panel -- perceptions of technology. And it's made up of people from multiple disciplines, everything from economics to IT, across all communities, academic, industry, and public governments. And they seek to look at things before they're actually put into motion from the committees -- from a community's perception, and actually see if they could identify issues that would come out and -- as things move forward with the technology that they're proposing. The ten-print [inaudible] biometrics that I think Mr. Paulson [sic] Mentioned -- is one of those areas that was actually brought before the panel and discussed fairly recently. And they gave us some really good feedback on how things might be, how there was room for improving things.

And, in conclusion, just hopefully I've kind of given you some food for thought or -- on how S&T, how Human Factors in particular, and S&T generally differs from other components in how they do research and how we are trying to -- within Human Factors in particular, because everything we do is people -- trying to come up with ways to work with the Privacy Office, with Privacy Officers, and the Civil Liberties Office to try and figure out how we can get further left of the process so that as we do projects we can either educate -- we can educate each other and hopefully mitigate or come up with

ways to change projects or add to projects, like synthetic data, use of synthetic data, use of anonymization techniques such as Mr. -- as Jeff was talking about earlier -- which he didn't mention that they were expensive to use, and Human Factors has a very small budget. But, that, you know, are ways and it's -- as it becomes even more, there seems to be generational differences in terms of our generation with the 20-somethings that are coming through now, in terms of what your expectations of privacy are and really when you need to draw those lines and how you can draw those lines so it's acceptable to everybody.

So, in conclusion, I just wanted to say thank you for taking the time to listen to us and we're really eager to try to move this relationship forward and see what we can do.

MR. BEALES: All right. Thank you very much. Our second speaker is Jennifer Schiller, who is with the Contractor, BAI, Inc., and is the Privacy Liaison and Deputy Program Manager in the Regulatory Compliance Office in the Science and Technology Directorate. Prior to serving as the S&T's Privacy Liaison, Ms. Schiller supported -- or, supervised the DHS-wide Human Subject Research Portfolio. She served in the U.S. Navy as a nuclear propulsion machinist's mate. She earned a Master of Arts in International Affairs from George Washington's Elliott School of International Affairs and a Bachelor of Arts in Interdisciplinary Studies from Long Island University. She is a member of the International Association of Privacy Professionals and holds the CIPP/G certification. Welcome.

MS. SCHILLER: Thank you. Thank you very much. We at the Science and Technology Directorate are very happy to be invited here today. We've been working very closely with Mr. Teufel and his staff, and we have made a lot of progress. We're excited to tell you about it.

We kind of went backwards with our S&T presentations. We heard from two specific parts of S&T and now I'm here to give you the wide overview, so hopefully those pieces will fall into place in the overall S&T puzzle.

I work for the Science and Technology Directorate's Assistant General Counsel for the Regulatory Compliance Office. And the goal of this office was to provide an independent compliance function that was not directly linked to any of the bodies within S&T that conduct research. So my office reports to the Assistant General Counsel; her stake is to ensure that our projects are legal. So the goal is to have independent determinations of compliance.

I'm here today to talk about S&T and our privacy compliance efforts. I'll start by discussing our mission, and then I'll move to an overview of our structure covering our six major R&D divisions, our three R&D investment portfolios, and our three R&D support and coordination offices. I'll close by discussing our privacy compliance initiatives and processes.

Our mission -- I'm not going to read this word for word; I hope you all have printouts, they're available outside on the table, but -- there are two main parts of our

mission. One is to conduct RDT&E, that's research, development, test, and evaluation on homeland security topics and technologies. The second part is to support our customers. Our customers are the other DHS components, some of whom you've heard from today -- ICE, CBP, US-CIS, Coast Guard; also our state, local, and federal law enforcement and first responders.

This is our authorizing legislation. We have the authority to conduct research. That is it. We can do RDT&E. We cannot do law enforcement, we cannot do intelligence, we cannot do operational activities. This is becoming increasingly difficult. Our customers are law enforcement, they are intelligence, and they are operational activities. So when they ask us to develop a technology, the only way we can go out and test that technology, prove its effectiveness, is to work with them in their operational environment. So it becomes a very difficult task to evaluate the privacy implications of those testing activities. Are we conducting research or are we conducting operations? Now, these are issues we tackle with the assistance of the Privacy Office on a day-to-day basis and a case-by-case basis.

This is an overview of our organization chart, and if I had a pointer I would point some things out to you, but I don't. At the top there you'll see our Under Secretary, Admiral Jay Cohen. All of our RDT&E activities are conducted under his leadership. Along the bottom you'll see our six technical divisions. These are aligned along enduring functional disciplines. They're linked to three research and development investment portfolio directors; those are the three individuals above that bottom row of six.

So the first two of our six research divisions, the first is Borders and Maritime Security; they develop in transition technologies that improve border and waterway security. They have three primary thrust areas; the first is border security. They're looking to improve the detection, tracking, and identification of threats along the border, to develop non-destructive tools to allow for inspection of hidden or closed compartments, and to assist law enforcement officers in ensuring compliance of lawful orders by non-lethal means. Second area is cargo security -- enhanced screening and examination by non-intrusive inspection, hardened air cargo conveyances, track domestic high-threat cargo.

Third is Maritime Security-- developing wide area surveillance, data fusion, and automated tools for command center operations, and improving ballistic personal protective equipment in WMT detection to improve officer safety.

Next, our Chemical and Biological Division. Now this is an example of a large amount of S&T research that, generally speaking, does not collect or use personally identifiable information. Here we're looking at developing tools to detect and mitigate animal disease breakouts, improve tools for integrated CBR and risk assessments, improve chem-bio forensic analysis capabilities, and develop handheld rapid biological and chemical detection systems.

Next we have our Command, Control, and Interoperability Division. Again, they have several focus areas. First, cyber security, information security, and also infrastructure protection. They develop interoperability communication standards and protocols for emergency responders. They work with the fusion centers very closely. So, if you attended the tour yesterday, our CID folks work very closely with those fusion centers.

Explosives Division develops the technical capabilities to detect, interdict, and lessen the impacts of non-nuclear explosives. They look at standoff detection; that's detection of explosives on persons at a distance. Capability to detect VB-IED -- that's very big improvised explosive devices. Capability to detect homemade or novel explosives, and optimizing canine explosives detection capabilities.

Infrastructure and Geophysical Division, again, they have several thrust areas. The first is incident management and the second is infrastructure protection, again. They focus on identifying and mitigating the vulnerabilities of critical infrastructure and key assets.

Our Human Factors Division is the next -- the final of our six major research divisions. You heard from Dr. O'Connor about the work of the Human Factors Division. They -- one of their focus areas that I find especially interesting is the ability to non-intrusively determine the intent of subjects during questioning and people screening. And so we have several projects that are focused on assessing a person's intent non-intrusively. The goal of these projects, believe it or not, is to enhance privacy. If we can tell non-intrusively that you are intending to do something bad, we can direct our secondary screening efforts at you and not at the people around you. So these are some of the projects we have that we hope to improve privacy even though the research process itself may involve collecting and handling personally identifiable information.

Our three investment portfolios, we have the Director of Innovation and Homeland Security Advanced Research Projects Agency, which we call HSARPA. HSARPA manages a portfolio of solicitations and proposals for the development of homeland security technology. They award procurement contracts, grants, cooperative agreements, and other types of funding arrangements for research or prototypes to both public and private entities. The goal is to accelerate the prototyping and deployment of technologies intended to reduce homeland security vulnerabilities. They work with each of our division heads to pursue game changing, leap ahead technologies that will lower costs and improve operational capabilities through technology applications.

We have our Directors of Research and Transition. The Director of Research coordinates across S&T to maintain a cross-cutting focus on basic and applied research. Each division has a section Director of Research who reports to the Director of Research. And the goal is to coordinate our research efforts and prevent duplications.

The Director of Transition coordinates within DHS to expedite the transfer and transition of our technologies from S&T operating in a research environment, to our customers in their operation a section Director of Transition that reports to that office.

Support and Coordination Offices -- we have our Office of Test and Evaluation and Standards. Their goal is to ensure objective testing in technologies and oversee standards development for interoperability being the primary goal there.

The Office of Special Programs coordinates highly classified projects executed by the six research divisions.

And finally are the rest of our support and coordination offices. The Office of Operations Analysis supports risk analysis and manages the Homeland Security Institute. They also are the home base for S&T's Federal Advisory Committee, the Homeland Security Science and Technology Advisory Committee, which we call the HSSTAC.

Our Interagency Programs Division facilitates government-wide science and technology coordination. We work with other executive branch agencies to reduce duplication and identify unmet needs and to help DHS tap into science and technology communities across the governments.

Our International Programs Division conducts science and technology outreach to U.S. allies and promotes international cooperation.

Research facilities -- the bulk of S&T research is not done directly by S&T. Most of our research is done by universities, by private sector vendors, by other government agencies, or by non-profit agencies. There are some exceptions; you heard from one of them, Dr. Hallowell, of the Transportation Security Lab. We also have the Plum Island Animal Disease Center, the National Biodefense Analysis and Countermeasures Center (NBACC), and the Environmental Measurements Laboratory. We also work very closely with the Department of Energy's national laboratories, Lawrence Livermore, Los Alamos, Sandia, Argonne, Brookhaven, Oak Ridge, PNNL; these laboratories also conduct research for us. So when we talk about S&T doing research, in most cases we're not doing research, we're funding research through contracts, through cooperative agreements, through grants.

And finally, our privacy compliance and awareness efforts. Now, this year we had our first annual S&T Privacy Day. We did mandatory annual training for all of our employees and contractors, and we trained about 2,000 people. We did an audit of all of our portable devices, thumb drives, portable hard drives, CD's, laptops, to try and reduce the amount of PII and ensure that all of our information was properly encrypted. And we did a file cleanup where we went through to minimize the amount of PII we store, delete, destroy any PII we no longer need.

Periodic data calls. I'm the Privacy Liaison from S&T to the Privacy Office, so I periodically will do data calls and ask programs to self-report on any projects they're

doing that may involve personally identifiable information. It's one of the ways that we have gotten up to speed with our compliance efforts. In the latest report, we were 100 percent on both PIA's and SORN's, so we really appreciate all the work the Privacy Office has done in helping us achieve that perfect score and we hope to maintain it.

Privacy compliance documentation. This is an area that we struggle with and will likely continue to struggle with. We are scientists and engineers; it is very difficult for us to get into the headspace of writing a PIA for the general public. We use big long words; we like to talk about our research in terms that only a handful of people can understand. It takes a lot of handholding to get us to produce a document that is understandable to a lay audience.

It's also difficult for us to step back from our programs and look at them in the light of privacy rather than homeland security. Our customers are very motivated by homeland security. Local law enforcement, for example, as you might imagine, privacy is not a big concern for your average cop on the street; school safety is. So, you know, we may be approached by a local school system or a police agency asking us to test a new camera system in schools. To them, that's a security activity, it's protecting their children; it's a priority. It takes some effort for us to step back and also look at whether the very obvious privacy implications of filming school children? So these are some of the challenges we encounter in working with our customers and trying to write privacy compliance documentation that meets the standards that the Privacy Office has worked to set for all of us at DHS.

Privacy Working Group. We do have an internal working group with representatives from each of our six divisions who report to me and work with me on all of the privacy issues and help me to set the agenda for what needs to happen in terms of policy and process improvements.

Dr. O'Connor mentioned the Community Perceptions of Technology panels, so these are managed by the Homeland Security Institute, which is in FFRDC, operated by our Operations Analysis Division. They mainly do risk assessment, so what they'll do is convene a panel of -- and step in if I go off here -- they'll convene a panel with experts, non-governmental experts, to look at a specific technology. They'll look at it in terms of privacy, civil liberty, anticipated reaction of your average Joe on the street. So they may take one of their screening technologies and just ask this panel of -- who may be lawyers or at local representatives -- ''What do you think about it? What bothers you about this? What are your concerns?'' And that's been a very helpful tool for us in understanding how to -- the public views our research and development efforts. I think there have been three rounds of that so far.

Collaboration with the main DHS Privacy Office. Our subject matter experts have provided input on efforts such as the Privacy Office's workshops on data mining and CCTV. We work very closely with the Privacy Office to plan privacy initiatives, such as our S&T Privacy Day; they participated in that and were very supportive of that. We're working with them now to develop some privacy principles for research. And

there are some areas where we could really use your help and expertise. We are approached by customers and by Congress to conduct research in areas that we don't know how to conduct research.

Domestic radicalization -- how do we look at domestic actors legally? You have -- Becky, step in if I go wrong here -- but is it (e)(7) of The Privacy Act, they can't collect information about the expression of an individual's First Amendment rights. So if I'm a member of a political group -- how are we, S&T, how can we study domestic actors with that restriction? Congress wants to do it; we don't know how. So these are the areas where we could really use some support and guidance from the privacy community on these issues.

Another, chemical plumes. If you were making explosives in your home, you will create a plume of chemicals that will rise up into the air and could be detected by you know, an airborne -- an air vehicle passing over. At what point are you violating the Fourth Amendment? You know, we have all kinds of thorny legal issues that we would love to have your assistance and support with.

Outreach briefings. I go to staff meetings for our internal divisions -- Human Factors, Explosives, Innovation -- and I talk to them about privacy, what they should look for in their research projects, the different type of privacy enhancing steps they can take. I have site visits. I visited the TSL several times. They have been very welcoming and receptive, and they are doing a great job on their privacy compliance documentation.

S&T policy development. We are working on developing policies to guide our internal R&D. It's a work in progress. As Dr. O'Connor mentioned, sometimes a project starts out with one set of goals and assumptions and by the time you get to the end you have an entirely different set of goals and assumptions. So it's a difficult environment to create policies in.

Participation in IPT's. Those are our DHS integrated product teams focused on various areas -- borders and Maritime, identity management. We participate in those and in project planning meetings to air privacy concerns early in the process. And then we coordinate across different compliance areas to ensure that privacy is tied in appropriately with Paperwork Reduction Act, with the FISMA certification and accreditation process, and with human subjects research concerns.

So, that will conclude my presentation. And we look forward to your questions and comments.

MR. BEALES: Thank you very much to both of you for being with us today. Neville?

MR. PATTINSON: Thank you very much. Very interesting presentations from both of you.

I've got a question about the HSARPA program. And I think you said that you fund -- you give grants and so on for this -- the investigations into technologies for homeland security and so on. In the subcommittee here and earlier today in the committee, we adopted a resolution to look at privacy questions in the grant-making process; do you have anything today in HSARPA that questions your applicants or your partners as you may have in looking at privacy specifically in that grant process?

MS. SCHILLER: I think the resolution, if I understand correctly, applied specifically to grants to the states; is that correct?

MR. PATTINSON: That's correct for that one. I'm asking for HSARPA now?

MS. SCHILLER: Okay. I just wanted to make sure I hadn't missed something. We do look at privacy with respect to our grants. Our grants -- our grantees do not complete PIA's at this time because the way our grants work is we will put out a solicitation that would say something like ''S&T seeks to fund projects related to homeland security.'' It would be very broad and very general. We have no involvement in the research process. We have no access to any information collected during the research process.

We would have no involvement in the collection of information, no access to the information, no governance over the R&D process itself; and in many cases, we may not get a formal report back. The goal of our funding of research is not necessarily to get anything; it's to further the development of technology in the private sector or in the government. So in many cases, we don't hold those people to -- they're -- because we're not directing the research, they're not held to the same standard as a contracted entity that is operating under our day-to-day guidance. Even our grantees -- our grantees do have to abide by the 45 CFR 46 policies governing human subjects' research. So anytime there is a human subject involved in any research, regardless of whether it's a grant or contract, that is reviewed by an institutional review board who looks at privacy, looks at the impact on the individual economically, legally, financially, socially, of the research. So we do have measures in place to assess the impact on individuals; they're just not the same measures that we use for other projects.

MR. PATTINSON: [Inaudible].

UNKNOWN MALE: Thank you. As you went through the overview when you were showing us kind of the glue that holds all the things together and you went through a broad range of issues, there was one topic that I didn't exactly see where it fit -- and it may fit across a number of topics. But is S&T doing any research related to pandemic planning and are they -- who are they coordinating with in the government? Because that's clearly a critical response that needs to be factored in also.

MS. SCHILLER: I believe we -- we have -- incident management may have been the bullet that you were referring to. And incident management is fairly broad. It would apply to any type of widespread incident, so it could be an outbreak, it could be a

natural disaster, it could be a terrorist event. The purpose of our efforts in incident management would be to coordinate first responders, to develop technologies to help first responders communicate, to develop technologies to help law enforcement officers measure the impact of an incident. But I'm not on -- I'm not in a research and development capacity myself so I'm not aware of any pandemic, centric research that we do.

DR. O'CONNOR: I believe our chem-bio department has something to do with that. They do sponsor modeling and simulation of the spread of influenza, and I believe they're working with CDC, DOD, and some institutions; like, I believe, like, Georgetown and there's a couple other places.

UNKNOWN MALE: Right. But if you think of the influenza, which actually Jeff Jonas raised as his suggestion and, I mean, at the time that influenza came out, it affected more than percent of the world's population and lasted more than four years. This is not a point-in-time incident response; this is a concept of institutional survivability and is a deterministic effect on homeland security. And so the question is, if homeland security is missing in action on the team that's looking at this, that's a problem.

DR. O'CONNOR: We're coming at that from an even broader perspective. We have within Human Factors, there's actually a program that does community resilience. And that's exactly the idea, is how -- to assume something is going to happen, and it might not necessarily be a pandemic, it might be any type of catastrophic event that would have long-range influences and look for how do you improve the resilience of the community and it's responses, both right after and over the long term? So, like, for instance, I think there is a project right now going on, PTSD, for survivors of -- I don't know if he's working with the Iraq veterans right now, the ones that did okay -- trying to look at how the ones that came back and didn't get PTSD survived and what were the coping effects that they had. So something as specific as that to something as broad as how do fusion centers link up with all the different other elements of the community hospitals, fire departments, law enforcement, to recreate a community after it's been obliterated?

MS. SCHILLER: And Dr. Hallowell also tells me that she's -- may be aware of an effort centered specifically on this within S&T. So we can get back to you with that information.

MR. BEALES: Joanne McNabb?

MS. MCNABB: My question was almost answered. I was interested in what sort of privacy or data security standards your IRB's is in, and if those are available to the public?

MS. SCHILLER: Those -- an IRB -- the IRB operates in accordance with 45 CFR 46; they have very specific lists of things they have to look at. We don't dictate the terms of what an IRB looks at, they follow their own institutions' regulatory guidance.

So the Department of Health and Human Services maintains a list of IRB's that are certified, and if an institution is working with an HHS certified IRB, then they are following those rules and regulations to the satisfaction of HHS, who is the regulatory authority for those regulations.

And they do a fairly broad assessment of the impact on privacy. They look at economic impact. If we're doing a study on, you know, something fairly sensitive, like people's attitudes about terrorism or attitudes about a controversial topic, could it have an economic impact on them, could it impact them socially if the results of this study were to become, you know, public? So they do look at a fairly broad -- take a fairly broad approach to privacy and do a comprehensive review of the risk and potential harm to human subjects that could come from the research itself.

MR. BEALES: Are there other questions? Well, then I want to thank you both for being with us today. They were very interesting presentations. We appreciate hearing from you. Do we know if there is any public signup -- public comments signups?

UNKNOWN MALE: I'll go find out.

MR. BEALES: Okay. That's the last thing on our agenda. The answer is no.

UNKNOWN MALE: No.

MR. BEALES: Well, in that case, I guess this meeting of the Data Privacy and Integrity Advisory Committee is adjourned. Thank you all for being here, and thank you everybody who participated to inform us where we weren't already well-informed. And I look forward to seeing you all in December.

MEETING ADJORNED AT 3:07PM.