Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Tuesday, March 7, 2006
Ronald Reagan Building International Trade Center
Polaris Room
1300 Pennsylvania Ave, N.W.
Washington, DC 20004

MORNING SESSION

MEETING MORNING SESSION: OPEN TO THE PUBLIC (POLARIS ROOM) MS. BECKY RICHARDS

Ms. Richards: Good morning. I'm Becky Richards and I'd like to welcome you to this meeting of the Data Privacy Advisory Committee. We will be opening our fifth meeting today, my name -- and I bring this meeting to order. We will begin first by turning off your cell phones and then Maureen Cooney, our acting Chief Privacy Officer and Chief FOIA Officer will introduce the Secretary of the Department of Homeland Security.

Ms. Cooney: Good morning and thank you. We'd like to welcome all of you today to the committee meeting and most of all, our committee members. It's an honor to be able to introduce this morning

Secretary Michael Chertoff, the Secretary of the Department of Homeland Security. The first time I had the opportunity to greet him was when he came to the department to speak to staff, and the auditorium at the Nebraska Avenue complex was lined and we stood in line to shake his hand. I missed that opportunity, I ran to the end of the line at the conclusion of his remarks. I think his security detail got a little worried, but he was very kind and I said, Mr. Secretary, the Privacy Office welcomes you. I remember him laughing and saying, very good, very good, I haven't had much privacy in the last few weeks. And I assume that has continued. It's a privilege to be able to say again, the Privacy Office welcomes you, as well as this committee, sir.

REMARKS ON THE DEPARTMENT OF HOMELAND SECURITY; THE HONORABLE MICHAEL CHERTOFF, SECRETARY

Secretary Chertoff: Thank you Maureen. I'm glad we got a chance to shake hands at coming in this time instead of going out. Well, I want to thank committee members for your hard work and advice as we continue to integrate our privacy protections into our programs and address privacy concerns in an environment which is probably one of the most challenging in government because our various elements interact with the public in a wide variety of settings and a lot of them do impinge on concerns about privacy. Some of the things that we've had the benefit of committee recommendations on, are the use of commercial data to reduce false positives in secure flight and other screening initiatives. And I certainly want to recognize Maureen for her tremendous leadership in terms of making this office effective and make its work significant. You know, privacy is really about -- we spend a lot of time talking about what privacy means. It actually means different things to different people. To some people it's about information management, keeping information confidential, having control over where information goes; for other people it's physical space, not having people intrude into your physical domain. And in some instances these various notions of privacy actually clash. One person's privacy is not another person's conception of privacy. There are cultural differences. You know, Europeans become extremely focused on the issue of data protection and they, frankly, are much more focused on data protection than we are. They're very intent on creating limitations of how long data is retained and they impose very strict conditions on how it's transmitted, frankly, more than we do in our law. On the other hand, in many countries in Europe, you have to carry national identity card and if you don't have it they can put you in jail or take you down to the police station. That would, I think -- certainly the requirement that you must carry a card or you'll be put in jail would just put Americans into orbit. So we have a conception of privacy that puts more weight on some things, they have one that puts more weight on others. And I think a lot of these are driven by historical examples and historical concerns. But as we go about doing our work, we really want to always bear in mind different conceptions of privacy, the different trade offs. People often talk about the fact that we need to trade privacy for security or that there's a trade off between privacy and security, and that may be true in certain respects. But I think it's also true there are different conceptions of privacy we have to trade off. One of the areas where I see this the most is in the issue of passenger screening. In a sense, right now we are heavy in physical intrusion, and also intrusion by way of questioning people, and light in terms of the amount of data we ask people to give us. And part of what we're trying to migrate to, I think, in our various kinds of screening programs is a regime in which perhaps with more information about people we would have to be less physically intrusive and we would have to question them less. So when we consider, is that protecting privacy or hurting privacy, I think the questions are going to be, well are there

different elements of privacy. Some are favored and some are disfavored under different regimes. So I think these are our tough questions we have to talk about and think about as we design our programs going forward. Of course, another element of privacy is information sharing. We are committed to an information sharing environment. In December of last year, the President issued a memorandum entitled Guidelines and Requirements in Support of Information Sharing Environment, which was an outgrowth of the Silberman-Robb Commission, which talked about the fact that we don't have sufficient information sharing as a embedded element of our operations among the various agencies that have responsibilities to manage information. And this, of course, has been a theme even of Congress which has in legislation spoken to the need to share information. And, again, when we talk about information sharing, we get to the issue of privacy and we have to then talk about what does it mean in terms of privacy? Does it mean that we have to restrict the amount of information that's shared or that we have to restrict the use to which it's put? This gets us -- gets us into such issues as Mission Creep, which is the tendency for information that's collected for one purpose to eventually be applied to other purposes. And I think we need to be very disciplined about the way we think about these issues and how we discuss them because I think that the more you get into them, I guess my thesis is the more you see privacy has a lot of different dimensions and some of them, in fact, are in tension with each other. And we have to be very clear about what are the benefits and what are the -- the harms as we consider issues like information sharing and environment and things of that sort. Clearly we need to be committed to better information sharing and the question is, how to we build protocols and regimes to make sure that that information is used appropriately and not misused. You know, one of the -- I don't want to ruminate too much, but one of the particular challenges is, how do we use information sharing to actually protect people against identity theft? In some ways a regime of better information sharing is more protective of people in terms of diminishing the opportunity for thieves or criminals or terrorists to steal there identities. So there again, what may appear in the first instance to be a challenge to privacy may actually promote privacy. Let me conclude before we throw it open to discussion with the observation of where the department is. We are still a very young and comparatively immature department. We are a little over three years old as we sit here today. And so we have a lot of opportunity to build into the sinews of this -- what I could describe as maybe an adolescent or young adolescent organization a respect for privacy and a thoughtful approach to privacy, which I hope very much this committee will help us do, and I'm looking forward also to Maureen helping us do that. I think we all know we don't want to live in a society where our privacy is regularly invaded. Heaven knows it seems to be invaded by private actors much of the time and we certainly don't want the government to become an invader of privacy. We want the government to be a protector of privacy and we want to build security regimes that maximize privacy protection and that also do it in a thoughtful and intelligent way. So, I think you all have

the opportunity to really be present at the creation of a culture of privacy in this department which I think will, if it's done right, will be a role model in Homeland Security, but a very good template for what government ought to do in general when it comes to protecting people's personal autonomy and privacy. So Maureen, that's my -- those are my comments. I guess we have a little bit of time for discussion.

Ms. Sotto: Thank you so much, Mr. Secretary. We very much appreciate your joining us. I'd like to ask the committee for questions please. Please put your name tags on -- up. Okay. Mr. Harper, please.

Mr. Harper: Mr. Secretary, thanks for being here. I appreciate hearing from you. One of the things you said piqued a memory of mine from the recent past when you talked about Europeans and their concerns about data. Obviously the European Data Privacy Directive represents a significant part of the data protection regime worldwide. But contrarily, Europe has also passed a data retention directive that will seem to require telecommunications firms to collect information for surveillance purposes for the use of governments. At Davos, the Financial Times quoted F.B.I. Director Mueller as wanting to implement international standards, among other things, pertaining to data retention. And I wonder if you're considering a U.S. data retention standard?

Secretary Chertoff: Well it's an interesting question. I don't know that anybody's proposed a specific standard. Generally speaking, my understanding is a lot data -- my understanding is that Europeans actually have pressed to minimized the amount of retention. The issue there is they've actually required that data be disposed of and eliminated. Here, generally data is kept for a long time and the issue is whether we can obtain the data or not through subpoenas or other kinds of means. An interesting challenge would arise if we -- if companies went to the business model of destroying data very quickly. Of course, they usually keep it for billing purposes. But if they would decide they wanted to destroy it very quickly, whether we would compel them to do more data retention. I think that would implicate two issues. One would be, of course, the financial issues in an unfunded mandate and, you know, we get some push back on that. The second is a privacy issue. You know, one of the proposals that was floated and shot down for a period of time, I think, before I got here, was the idea of having screens for protection. Instead of the government actually retaining data and collecting it, letting private parties keep their own data but let us -- letting us run screens against the data, submitting a name, having it pinged against a private database, and then have the private data holder who has the data anyway go yea or nay, red flag/green flag. And only if it was a red flag would we then get the underlying data. So that -- that might be a model for some kind of data retention issue. It might be one that would say the government, instead of holding the data itself, would allow it to remain the private sector, provided the private sector retains it for a period of time so we can ping against it. This comes back to my basic,

I guess underlying thesis. It's too easy to say something is pro-privacy or anti-privacy. On a lot of these issues, actually, are putting security totally aside. Some of the proposals we -- that we encounter actually are simply trade offs on different elements of privacy. It may promote privacy in one respect and may diminish it in another, or it may impinge it in different ways. And that seems to me to require a deeper analysis of the trade offs. In this case, a requirement of data retention in a private sector might be seen as being anti-privacy, and yet, if that led to the government having less information and keeping it more in the originating private hands, people might say that protects privacy. So I think you got to ask yourself with specificity what actually privacy objectives are served or dis-served by a particular proposal.

Ms. Sotto: Thank you. Forgive me if I'm not calling on people in exactly the right order. This seems like a race to the finish to put up your cards. Mr. Alhadeff.

Mr. Alhadeff: Thank you. And thank you Mr. Secretary for joining us. I wanted to actually pick up on the theme that you just last mentioned, which was that kind of concept of the privacy trade offs. In your earlier comments you had talked about the concept of more or less intrusive as part of the airport questioning and things of that nature. And I guess I wondered what you thought about -- because I think most people would agree on the less intrusive but would also want to have an awareness so they would be able to judge reasonableness of the questioning. And I guess there's a fear that when things get taken out of the direct interaction there's less of an ability to judge reasonableness. Are there any mechanisms that the department can use to help people get a better understanding of the reasonableness and the nature of the questions and benefits that accrue to them?

Secretary Chertoff: I'm not sure -- do you mean questioning when people are directly questioned at the airport?

Mr. Alhadeff: Well if you're shifting from questioning to a screening process that is perhaps less evident to them, they can judge the reasonableness of the questions. The screening is a little harder for them to judge, and I think for a lot of people there's the question of the transparency of what's done with the information and how.

Secretary Chertoff: I mean -- well, part of that is we have to have redress. I mean, there are obviously mistakes. But here, again, you know, there's a funny issue with trade offs. To the extent that we are only able to obtain names from people and we're not -- when we get ticketing information we don't, let's say, get date of birth. The name is a very blunt instrument for screening, and that leads to a lot of false positives, and that leads to the stories you always hear about -- about 11 year old kids being questioned because they have the same name as somebody who's on a terrorist watch list. That is very, I think, counterintuitive and distressing to people. If you got more information, date of birth, address, none of which is a super secret, you will really be able to screen out an awful lot

of people from being stopped and questioned. Now, I think actually most people would prefer that, particularly if we explained why we're doing what we're doing. And that's an example of what you said, where we can make it clear that -- and that's not very sophisticated, it just -- it just creates finer screens for separating out people that we're interested in and people that we're not interested in. As we get further down the line, you know, you start to ask questions, are there other things we could ask that would even allow us to expedite the travel process for more people, requiring even less people going into secondary and things of that sort. One solution to this might be voluntary systems, what we call registered traveler systems. Where, while it wouldn't completely eliminate your physical screening, your identity screening would be taken care of if you enrolled in registered travel and you had a biometric card and we did a check. And that's a -- that's a market-based or voluntary-based system. So that's another way to approach the problem, I think.

Ms. Sotto: Thank you. Mr. Barquin, please.

Mr. Barquin: Again, thank you for being here, Mr. Secretary. One of the -- of the things that, in this drive for information sharing, we believe will be critical and it will raise a number of privacy considerations also, but has been lacking has been the ability to share information with the first responders, just cross levels of government. And a significant part of that, I think, a necessary precondition is the question of trust, trust up and down. And the question is, specifically, what is the department doing to try to increase that level of trust between governments.

Secretary Chertoff: Well a lot of what we're doing through our information analysis, intelligence analysis, intelligence and analysis component is to share both in terms of our internet and our secure internet to actually imbed some of our officials in state and local and bring some of them into our operations center precisely to increase this level of trust. There are always two elements to information sharing. One is trust, which means getting people at appropriate security clearance or background check. The other is, of course, need to know, which the less often commented element. And sometimes people, even when they're trusted, don't get information if they don't have a need to know. That's good security practice. I know people get offended sometimes because they think if they've been cleared they should be able to see anything. But, I can tell you that even among people who have the highest level clearance you can get in the government, you still don't get information, and you shouldn't get information, not pertinent to your job. So there's always a need -- a reason -- you have to justify why you get information in terms of your job function. That's, by the way, another good example of protecting privacy as well as security. I guess my thesis here is that the simple privacy versus security balance we often here about is simply way oversimplified. That in many ways, these things serve common interests and that it's much more complicated. Bottom line is

we're doing a lot to try to increase the networks through which we communicate but we also have to remind people that in the end, people get information because they can use it, not merely because they want to be in the know or satisfy their curiosity.

Ms. Sotto: Thank you Mr. Barquin. Mr. Purcell.

Mr. Purcell: Thank you Madam Chair. Mr. Secretary, thank you for joining us this morning. I noted with delight, I think, and I share by most of the committee members that you mentioned the government wants to be a protector of privacy, we certainly support that, and that your interest this year in developing a culture of privacy in the department. Part of that culture has to be based on leadership. I think the committee would be very interested in hearing your thoughts about filling the vacant position of Chief Privacy Officer and in the department it's a -- a position that we all have a very fond attachment to, not only the individual filling the acting position in Ms. Cooney, but also in the long term prospects of making sure that leadership is not only filled, but also really firmly supported over time.

Secretary Chertoff: Well, we do support it. I mean, the process of filling jobs is one that's often lengthy because we do look through a lot of candidates. We want to make sure that, you know, even if we have people in place who we could promote, we also want to look outside to see if there are other candidates and then the prospect of your background checks and things of that sort. So we do -- we are focused on this position and more than that, we want to be focused on it not as a component that's a stand alone, but we want to have it be an issue that we talk about even in all of our regular activities. I think leadership is not just having a Privacy Officer and say okay, here's your Privacy Office, go deal with privacy, but it's treating privacy as an element of everything that we do. And I can tell you that we often discuss these issues and have discussed these issues with counterparts in other countries as we -- as we consider how to devise our programs. So we look forward to continuing to interact with the Privacy Office, both in terms of their perspective, but also because we want to get general good advice on how to work privacy through everything that we do.

Ms. Sotto: I have just gotten the nod that the Secretary needs to move on to his next appointment. Thank you so very much for joining us, we appreciate it.

Secretary Chertoff: Thank you very much. Thanks a lot. Thanks for your fine work.

Ms. Sotto: It was a privilege to hear from the Secretary directly about his view of privacy and also very heartening to hear that he considers privacy a priority on his agenda. I'd like to please ask Maureen Cooney, the acting Chief Privacy Officer to address the committee. DHS PRIVACY OFFICE UPDATE, MS. MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER AND CHIEF FOIA OFFICER, DEPARTMENT OF HOMELAND SECURITY

Ms. Cooney: Thank you very much. Lisa, if it's fine I'll speak from this chair. It's a pleasure to be with the committee again and to report on the activities of the privacy office. What I'd like to do today, given the short amount of time we have and the very packed agenda that you have, is to focus on three main areas that we've been working ardently on, not just since the last committee meeting, but actually for quite some time. And because the focus of the meeting today is on information sharing, both within DHS and externally, I'd like to first speak to that issue. Since the 9/11 Commission report, as well as since the passage of the Intelligence Reform and Terrorism Prevention Act of 2004, the privacy office at DHS has really taken a leadership role on an interagency basis in helping and in assisting and building an information sharing environment. That's what is required by the law. And some people call that a need -- a move from a need to know atmosphere to a need to know and a need to share information atmosphere. We've taken the position and have had the full support of the Secretary and of everyone, actually, at DHS, that in moving to this need to know, retaining that, but also need to share, we need to build in important privacy protocols into the way that we share information from agency to agency and from first responders. Ken Mortensen of our staff has, in particular, been heading up this effort within the privacy office along with very helpful legal counsel from our chief counsel to the privacy office, Elizabeth Withnell. Some of those achievements to date have been making sure and participating in the language of the Executive Order and the memorandum to executive offices that the President put out in December on information sharing. That directs every agency to look at both privacy and information security in the way that we share information across agencies and with first responders. Every agency is asked now to internally look and provide guidance within their departments on how that can be achieved and there will be a coalescence of -- between agencies. So we're actively engaged in that activity. There are many working groups that are working on that and it's been a top agenda item for the President and, I can tell you, for DHS The second item that I'd like to talk to you a little bit about would really be in the sphere of technology, in information sharing both, again, within the agency but also with our first responders, with other federal agencies, in order to allow people to move back and forth for many screening purposes. I know that that is a particular focus for you. In that effort we have spent countless hours working and advising with in the department and with other departments as well on two specific programs, Real I.D., the implementation of Real I.D., and the U.S. Pass program that would allow travelers to move across Mexican and Canadian borders, over our border into Mexico and Canada and back and forth. Specifically, the issues that we've looked at, and I've, of course, I'm abbreviating this, we have had a long list on which we've given guidance within the agency, but specifically we've looked at how technology is used, what we can do to better utilize technology in a safer way to protect information that would both protect the identities of individual travelers, keep their information from being scanned inappropriately, and at the same time, give enough information to our

border protection staff so that they're able to facilitate that movement across borders. Finally, I'd like to report on, again, a major priority in the office since the time that the office has been set up, and that's on partnership and dialogue with our international partners. A great focus within the department is on immigration and on visitors who come to our borders and come here for very peaceful and good and beneficial purposes both to Americans and to our foreign visitors. To facilitate that, though, because of differences and approaches to privacy and understandings, even of our laws here in the United States, of how we protect information, we spend a good deal of our infor -- of our time and efforts on dialogue with international partners. Most recently, we've been to Europe, we've been to Asia, to the APEC conference most recently, and the Secretary himself will be doing the outreach very soon, in the near future, with many of our international partners on these issues. I'm happy to be here and as we take breaks and have time together I'm very willing to answer any questions you might have. I might also direct you to our most recent addition of the Privacy Matters newsletter that brings you up to date a little bit from the fall until now of progress within the -- within the Privacy Office. And I want to emphasize, as I try to each time we gather, that our efforts in the Privacy Office are not done alone, just as Secretary Chertoff mentioned. It is in partnership and collaboration really with every office within the department and with the full support of the Secretary's office. And so I'm glad to be able to report that to and I thank for this time.

Ms. Sotto: Thank you very much Ms. Cooney. Thank you for your remarks. I'd like to ask if the next panel is here and ready to begin a little bit earlier. We've got one, are both here? Okay. Why don't we take a short break, about -- sure.

Ms. Richards: Good morning. I just have a few administrative matters. If you would like to provide comments during the public comment period, which is scheduled to begin at 4:30 this afternoon, please sign up on the sheet with Lane Raffray who is at the back of the room and give them your name so we can call you up at that time. Also, I would like to remind the committee members, as well as the panelists, to speak into the microphone so we can make sure that we record your statements accurately. And, again, if you have your cell phone or beepers on, please turn them off.

Ms. Sotto: Okay. Why don't we take a few minutes while we wait for our second panelist on our first panel this morning. Why don't we reconvene here in about ten minutes. Thank you. (Off record)

Ms. Sotto: I'd like to ask everybody to get seated please. Thank you, and thank you for our first panel of the day for seating themselves. I'd like to remind everybody on the committee and on the panels to please speak into the microphones. We want to make sure that we're accurately recording your remarks. Our first panel is -- consists of Betty Chemers and Dr. Herb Lin. They will be discussing a report that is being prepared by the

National Academy of Sciences. And I will let them do the honors of describing that study in great detail. But the quick summary is that this study is intended to address the information needs of the government in light of the challenges of terrorism prevention, and that specifically will examine the nexus between terrorism prevention, technology and privacy. I'd like to introduce both of our speakers and then ask you to go forward. Betty Chemers is a senior project officer at National Academy of Sciences. Prior to joining the academy she spent 30 years in the public and not for profit sectors working on criminal justice and juvenile justice issues. Ms. Chemers is responsible for the NAS study on the technical and privacy dimension of information for terrorism prevention and other national goals, that's a mouthful. This was a study funded by the National Science Foundation and by DHS.

Dr. Lin is a -- is a senior scientist and senior staff officer at the Computer Science and Telecommunications Board of the National Research Counsel of the National Academies where he's been study director of major projects on public policy and information technology. Dr. Lin's work includes a 1996 study on national cryptography policy. Prior to his NRC service Dr. Lin was a professional staff member and staff scientist for the House Armed Services Committee. Thank you, you have the floor.

NATIONAL ACADEMY OF SCIENCES STUDY: TECHNICAL AND PRIVACY DIMENSIONS OF INFORMATION FOR TERRORISM PREVENTION AND OTHER NATIONAL GOALS (PREVIEW); MS. BETTY CHEMERS, PROGRAM OFFICER AND MR. HERB LIN, SENIOR SCIENTIST

Ms. Chemers: Thank you very much. There was a very brief summary of this study that was made available, I gather, to the committee, and there are copies on the table outside. Let me -- let me begin very -- with sort of a caveat. This is a study that is just beginning. Our committee is in the process of being vetted. The first meeting of the committee will take place on April 27th, 28th here in Washington D.C. So our committee has not yet met and what we will be talking about a little bit today and describing for you is the statement of task that has been developed in conjunction with our project officers at the Department of Homeland Security and the National Science Foundation. So with that caveat, let me just provide a little background and then talk to you a little bit about what -- what we hope this -- what this study is and then, really, I'd like to spend some time posing some questions to the committee members because you have been involved in lots of different issues that certainly have some relationship to our current study. As was mentioned, this is a joint project, actually, of three different parts of the National Academy of Sciences, the Computer Science and Telecommunications Board, which is in one division of the Academy, the Division of Engineering and Physical Science, the Committee on Law and Justice, and the Committee on National Statistics, both of which are on the Division of Behavior and Social Sciences in Education. For those of you who are

not very familiar with the National Academy of Sciences, we've been around for a long time, in fact it was President Lincoln who chartered the national academies. He was in need of some advice, the story goes, about the ironclad ships and whether they were actually going to sink. So we've been around for a very long time. Our studies are funded through, there is an endowment, but they're also supported by federal agencies who seek really independent advice on particular topics. There are three components: the National Academy of Engineering; the Institute of Medicine; and the original National Academy of Sciences. Two of these components primarily do their work through the National Research Counsel. The membership of the academies is elected and it is the -- it is a combination of the members of the academies and experts throughout the country who participate in our studies. They are un -- they are unpaid and they are supported by very well educated, competent staff at the National Academies. This is my first study; this is my maiden voyage. Dr. Lin has been study director for a number of other studies. The study is unusual in that it represents emerging, first of all a collaboration between very separate divisions of the academy, although that has been done in the past, but the background to this study, it's actually a merged study of two separate studies that had been individually funded, one by the Department of Homeland Security that was really focusing primary -- focusing to a large extent on information for terrorism prevention and balancing that need for information with privacy. At the same time, Dr. Lin's committee had received funding for a study from the National Science Foundation to look more broadly at the technologies the government was using, primarily technologies involved in access to large scale databases for the purpose of terrorism prevent, but also for other national goals, law enforcement, public health. And there was also -- there has also been an interest in our study from the National Statistical Agencies who are somewhat concerned that the various discussions and controversy around privacy will really affect their ability to collect information. And so they are also a contributor to this -- to this study. The -- how the study works is, as I said, there is a committee that's convened, it represents national experts and they will be holding, over the next 18 months, a series of meetings. There will be three in -- three in 2006, probably two in 2007. And they will be developing the report during this period of time. Our studies are consensus studies. There is a real attempt to develop consensus among the committee members. This doesn't always occur. There is rarely -- sometimes there is a dissenting or a non-concurring opinion. But that is very -- that is really very unusual. Once the report is generated, it is fed through a peer review, a review process that involves sometimes dozens and dozens of people. The government -- while the government supports this study, the government really does not appoint people to the committee. It can suggest membership. And the government really does not see the report until the report is completed. Let me talk a little bit about the study -- the study itself. It was mentioned kind of the overall goal and it's kind of looking at the nexus between terrorism prevention, technology and privacy. What we are trying to do -- we are a science-based organization, and basically one of our

focuses will be the quality -- the quality efficacy of the technologies that are being -- being used. And I think that in some ways sets our study apart from other studies -- other reports that have been issued around this -- around this top -- around this very, very important topic. And I noted that there are people on the committee who participated in the Markle Foundation study and in the Tapac study. So, one of the ways that our study really does differ, is its emphasis on technology and the quality of that technology to, first of all, provide information that is going to be useful to the government, and then to look at what the issues are involved -- and technologies not only providing the information, but the technologies that are actually ensuring privacy of the data. So, on our committee we will have people who are experts in encryption, in data mining, in information fusion. We will also have experts in privacy and security law. We have someone on the committee who has a public health -- who will have a public health background, a law enforcement background. So it's -- in some ways it's much broader in terms of its scope, but it is also really narrowing down to the issue of the uses of the technology and how good is -- how good is the technology that we've all -- we've all been talking about. There are really -- our statement of work really is described in the summary, really focuses around four major tasks, but I have to say at the first meeting of the committee in July -- in April, one of their first tasks will really be to focus even more on this statement of task. It is a very broad statement. It talks about examining surveillance, data mining, and information fusion to determine what technological standards exist and what can be done to develop a stronger empirical ground. It's to look at -- we have been requested by the Department of Homeland Security to specifically focus on available and emerging surveillance technologies. By that we're talking specifically about such technologies involving cameras and what has come to be known as deception detection. We are looking at privacy and other issues affecting cooperation among government and private organizations. And then we've also been asked to look at research around public opinion and basically what really can be done to ensure that the public kind of understands what the government really is doing here, the needs that it has, and what is really being done to protect privacy. So there are a lot of questions that this statement of task really could -- could be developed. And that is actually the first order of business for the committee -- for the committee in April. I neglected to say the committee, because this was two studies that have been merged, the committee actually has two co-chairs, Charles --

Dr. Charles Vest who's President Emeritus of M.I.T., and Dr. William Perry, former Secretary of Defense under President Clinton. Let me turn to Dr. Lin right now and ask if he wants to add and -- or, just, no?

Dr. Lin: I couldn't have done better myself.

Ms. Chemers: Whoa, that's high praise from Dr. Lin for me. We can throw it open to questions, but I actually have some questions for you. But I'll - - since I'm your guest I'll give you a chance to ask some questions first.

Ms. Sotto: I'm looking at the committee. Questions please. Yes?

Mr. Hoffman: Yes, thank you very much for being here. I'm intrigued by the phrase that you mentioned - deception detection?

Ms. Chemers: Uh-huh. (Affirmative)

Mr. Hoffman: And wanted to frame my question about exactly what you mean by that with more of a comment. At one of our meetings last year, the meeting that we held in Bellingham, Washington, Deidre Mulligan from the Samuelson Law Center was one of the folks who came and talked with us. And she talked and raised the issue that what she believes that we need is -- and I'm paraphrasing, a much greater discussion of what the reasonable expectation of privacy is for individuals when they are in public spaces, specifically with regards to the myriad of technologies now that can collect information in those public places, but particularly with the dramatic increase in the use of cameras that we're seeing. When I read through the materials it makes specific reference to the London experience and I thought that was very interesting. And I wanted to get your thoughts on how the study might address that issue of what the reasonable expectation of privacy is in a public setting for individuals and how the use of cameras may impact that. What is actually being referred to by the London experience here and how that fits into this idea of deception detection? Many part question.

Dr. Lin: Since you've turned your name card around, we can't see who you are, so it would be helpful to know...

Mr. Hoffman: That's my privacy.

Dr. Lin: Right. I know -- (inaudible).

Mr. Hoffman: David Hoffman.

DR. Lin: Great, thanks.

Ms. Chemers: That's got a -- I think that the expectations around privacy are -- is probably one of the most difficult issues to really address. And the issue of privacy in general, in fact Herb can talk about this, has been the topic of an entire other study that's currently coming to conclusion at the National Academy. Maybe Herb, you want to just talk to that -- speak to that right then.

Dr. Lin: You finish what you were going to say and then I'll...

Mr. Chemers: Okay. The issue of deception detection -- we're using that as a -- as a phrase really to describe a number of technologies that come under that, which we know

that the Department of Homeland Security is quite interested in and, in fact, has been sponsoring some research on: facial recognition; the whole thermal imaging; and of camera surveillance. The London experience was mentioned specifically because that is, obviously, the best known example of cameras being used to identify perpetrators of the violence in London and they probably have the most -- have had the most experience in London, generally. They've been using it for crime control for probably at least eight years and they've done some studies on it. There's also work going on in Canada. So that's why it was mentioned, because we're really interested in rev -- in looking at what do we really know about the uses of this technology. So that's -- that is the reason that it's -- and there is -- there really is some documented evidence of the use of cameras in London. So I guess, in terms of the reasonable expectation of privacy, I don't -- I really don't know if the committee -- if this particular committee will kind of take that up or whether -- and in what form they will really address it. But I agree, that is -- it's a -- our notions of privacy have really -- are changing. And they're - - not only are they changing here in this country, worldwide they differ from one country to another. So it is a very complex -- very complex issue. Herb, do you want to speak about the privacy?

Dr. Lin: Yes. There is another -- you should know that there is another study that's -- that my unit is undertaking on privacy in the information age. That is a study that was chaired by Lloyd Cutler and William Webster. And we've had a certain amount of difficulty in completing this study because of a certain unfortunate event about one of the co-chairs, as you know. But, nevertheless, we are hoping that that report enters the review process sometime in the next few months or so. That report is intended to provide a framework for thinking about privacy in the information age and one of the reasons that I have that project is to help act as a liaison between that project and the current project that's being talked about. And we think that that project will provide at least a point of departure for the present committee to -- in its deliberations. Apropos of your comment about -- specifically about reasonable expectations of privacy. That issue is, in fact, part of the study that we're undertaking. I can't tell you what the committee is ultimately going to say about that. I don't know yet what it wants to say about that. But I can tell you, obviously, some of the things -- it is a complicated issue. It's -- reasonable expectations of privacy have both descriptive and normative components to it, what should -- what should be the reasonable expectation of privacy and, of course, once you put the word should in, you put in all kinds of issues about context -- social context and so on. Should you have a reasonable -- a greater expectation of privacy in a -- in times when we are threatened versus unthreatened? Well, that's an interesting question. Obviously technology -- the available technology matters in that too. I think what will come out of this -- our report will be a discussion of the factors and ways of thinking about it, but it's hard for me to imagine that we'll say the following is what we mean by reasonable expectation of privacy as a pronouncement. It's hard for me to imagine that we'll say that.

Mr. Hoffman: Just one follow up comment is that I would encourage you as you meet to scope exactly what this new study is going to be to think about the reasonable expectation of privacy as one of the sub-points within your quality discussion, that, in my opinion, quality has to be viewed as whether the individual mechanism or device is relevant for the defined purpose for which it's being used. And that defined purpose, I think, is often what gives rise to what our reasonable expectation of privacy is because it is context specific, as Dr. Lin was mentioning, it depends upon the individual situation that you're in and what other interests the individual has. But I think that would be very helpful to us if you could -- and I think very helpful to the overall privacy discussion.

Ms. Sotto: Thank you Mr. Hoffman. I would just add a little bit to that, to think about the appropriate use of information as well. Because I think the appropriate use will differ based on context, based on societal concerns at that given moment. And I would also ask Dr. Lin if you need any help or would like further discussion with this committee with respect to your study in particular and I'm -- I would ask the same, how can we help you, with respect to the other -- the bigger study. But your study seems like it's much farther along, so if we can help you in any way we'd be delighted to do that.

Dr. Lin: You may regret making that offer.

Ms. Sotto: I'm sure we won't.

Dr. Lin: Okay.

Ms. Sotto: Tara Lemmey.

Ms. Lemmey: Well as a -- as a technologist from Silicon Valley, I caveat this by saying it's been -- and as a member of the Markle taskforce, as well as this committee, what we've found and what I've found through the years is that if you think it, we can build it. So looking at the narrow definition of technology as your mission statement I find it sort of interesting and perhaps challenging because the technology has to live within business rules and processes and the culture in which it's going to be implemented, which I think are significantly greater problems than the technology itself, given that the technology can be adjusted pretty much in any way to achieve any means. And frequently there are non-technology means for solving the problem. I'm wondering how much you guys are anticipating that and how are you going to explore those business processes and rules and the cultural aspects that go into this?

Ms. Chemers: Well, one of the big issues for us in our discussions, even planning our first meeting, is the issue of how -- and to our committee will be how much do they want to get into the operational issues, because they are very important, but I think that is -- I think that is really going to be something that they are going to need to really talk about. And whether they can in fact be focusing -- be limiting their conversation and their discussions to the technology itself or the -- the use of the -- the operational use, the

problems that occur, when in fact they, you know, they're employed. So I don't know, because it -- it will really depend.

Ms. Lemmey: Well, the technology itself is transitory, short-termed -- lived, very malleable, adaptable, could be anything. So it's sort of, I would highly encourage the committee to go beyond that, because the technology -- studying the technology at any given point in time is arbitrary, random and can change within three months. And so it could easily be a completely different set of discussions if you focus on the technologies as opposed to focus on the uses and the processes. I just strongly encourage that.

Dr. Lin: I don't think that there is any question that the -- you know, that the latter part is right, that you have to focus on potential uses, but different -- we have to conceptualize different ways of achieving the same goals and -- there's no question about that. At the same time, I think I would take a little bit of issue with your statement that technology can be -- can do anything and, you know, we can discuss that offline if you want, but there are -- you're certainly correct that there are -- that assuming a static technology is the wrong way to go. If that's what you're trying to get us to realize, you're absolutely correct and we certainly don't believe that. And, as Betty says, some of the operational constraints, the real world constraints on this, business processes and rules and so on, absolutely an important part of the study. So no disagreement there.

Ms. Sotto: Thank you. Just as a slightly illustrative point, yesterday during the emerging applications subcommittee meeting, we talked -- we were talking about RFID, but we had some guests from DHS come in and talk to us about the uses for RFID and the potential uses of RFID at DHS, and they used the term automatic identification and data capture and said to think of that rather than RFID in particular, because RFID is just one of many, many different technologies that can serve this purpose of automatic identification and data capture.

Mr. Turner?

Mr. Turner: Thank you both for being here and I'm very intrigued by the studies that have been fused and I look forward to following them over time. I realize that you're early along in the process and this may not be a fair first question, although there are three parts to this, so one may be more fair than the others. First of all, I'm -- in looking at this summary that you've provided, I noticed you do have a scope of work, but I'm wondering if you could perhaps help me articulate or understand better the objectives of these studies, which I would I would distinguish between the scope of work and the objectives, because it's not at all clear to me. For example, in your first sentence where you talk about addressing the specific information needs of the government as it faces the challenges of terrorism, are there unmet needs that you've identified that you're addressing or is it just needs in general? And then, in the second sentence in your scope of work, this actually would be very helpful to the committee, as we debated this point

yesterday, this notion of surveillance, how do you differentiate between surveillance, data mining and information fusion technologies? Wouldn't you consider -- do you consider, for instance, data mining and information fusion [to be] surveilling technologies or not? And then, finally, in your third component of this, the fact that you're developing a framework, it looks actually very suspiciously similar to a framework that this committee has been laboring on for the better part of six months now, and I'd just like to raise -- bring your attention to a document that we will be voting on today and suggest that you consider that. We certainly won't even charge you for that advice.

Ms. Sotto: And I would invite you to sit through the discussion of the framework document later on this afternoon if you'd like to join us.

Dr. Lin: Let me answer the -- what I think is the easier question there, your number two...

Ms. Chemers: Thank you, Herb.

Dr. Lin: ...is surveillance and data -- or data mining and information fusion part of surveillance. There is a good argument that they are. I think that what we were talking about -- just as a definitional term, just so we have a way of talking about it, that surveillance technology is referred to the acquisition part of it and the data mining and information technologies refer to the analytical part that you might do there. In terms of the purpose of the technologies, it's all surveillance in some sense. You want to find -- you collect data, you want to find things in that data. It's obviously not useful to collect data if you're never going to look at it and so on. But it was just a way of talking about. There -- please don't read too much into the distinction between -- the fact that we use different terms for that. Betty?

Ms. Chemers: Thank you, Herb, for answering the easier of the three questions. I -- the -- your first comment on what information needs, I think that is going to be really one of the first tasks of the committee. And it's going to obviously be a question that they're going to have to pose to DHS: What information are you using, and I guess the companion question to that is has this information proved to be helpful? Now that gets us into some pretty protected waters, I think. But I think the question does has to be -- does have to be asked, and we are -- this is -- some of our studies, you know, are done by people who have security clearance and really have access to top level information. We will not -- our committee will not function that way, although we are hoping there are several who have clearance and perhaps will be able to delve more deeply into the uses of the information. But clearly that's the founda -- that's the foundation for the study. And these -- I mean the study is prompted by the growth and use of the new technologies to provide information and really, is this information being effect? Is it being used and is it effective? So it's a difficult -- it is a difficult question to answer. Terms of framework and the use of the word framework, I have to plead here -- our scope of work -- I mean,

generally, we prepare these in a kind of a broad way, they have to go through many levels. On the one hand, they can't be too specific, but I think the key here is what is this report going to really look like when it's done and who is it going to be useful for. So it may be, even in using the word framework, we sort of argued among ourselves whether that was a very useful word and what do we really mean by framework. So I think really the more important issue is what I just described, what is this report really going to look like and who is going to -- who is it going to be useful for. And we have an interest in having our report be useful for the government and so it is something that we will continue at each meeting, continue to raise who is the users of this report. And that's really the question we focus on as opposed to well, what's a framework. I mean it's useful to have a framework so you can look at other things, but I don't -- I would be surprised if, in a way, it's duplicative of the framework that you're describing.

Dr. Lin: One -- just to follow up on a comment regarding the specific information needs. We do understand that from the standpoint of people doing intelligence and so on, everything might be relevant. There is -- it's hard to imagine a piece of data that would be impossible to be relevant to one of these investigations. We understand that. And we also understand, on the other hand, that the safest thing to do about protecting privacy is not to collect data in the first place. Okay? We understand that tension, and it's a very real one that will inform most deliberations on the committee. We do understand that and, you know, we just have to see how that one plays out.

Ms. Sotto: Thank you. Mr. Alhadeff?

Mr. Alhadeff: I guess mine kind of builds on the previous two questions to a certain extent. And it may well be -- the limitation I have is the abstract of the committee's mission, a very abbreviated version of what's actually going to be going on. It seems like, where it's looking at technology, the major focuses are on the effectiveness of the technology in terms of integrity and quality of information, as well as the procedures that one may want to place around the technologies so it is perhaps least intrusive or most respectful. In terms of, kind of, maybe Tara went a little far in saying if you think it, you can build it...

Ms. Lemmey: (Inaudible).

Mr. Alhadeff: ...but the -- the question of the ability of technology to serve multiple purposes, one of which is, for instance, the respect and implementation of privacy policies. And I was just wondering whether there is a portion of your looking at the technology effectiveness to see how effective it is at actually implementing some of the policy issues that are around it. As an example, a database has tons of security technology. If one thinks about it, one can implement that security technology to also optimize privacy because access controls can be optimized on a need to know basis and things of that nature. If you only think about security, all you may think about is keeping outsiders out

and insiders in. So I'm trying to figure out, is there an element in the study that's also looking at the effectiveness for the usability of technology to optimize both, what the function is, which maybe surveillance or monitoring or data mining or whatever, but also what's its functionality for maintaining privacy or assisting privacy, not taking the place of policies, but perhaps supporting them.

Ms. Chemers: I think that's a valid point and I think that's an important point for the committee to consider, and we'll raise it. Thank you. It's a very...

Ms. Sotto: Thank you Mr. Alhadeff. Mr. Hoffman?

MR. Hoffman: Thank you. In your study -- in your studies I hope you will consider developing and using and arguing about metrics, public metrics for the advocacy of programs, for the privacy, for, if you will, a barometer of well being which can be viewed from the viewpoint of several different players because it may be that, depending on how something is implemented and what actually gets done, it may be great for public policy player A and not so great for public policy player B, but if, in developing your framework or your context, you actually have something that's at least halfway measurable, even if it's in terms of a fuzzy metrics of some sort, it'd be, I think, potentially useful to look at because right now we really have a lot of words, but we -- that's all we have. We don't have really good metrics on this right now.

Ms. Chemers: I think -- I think you're correct. That's a -- there really has not been a lot of work done in this area as I'm preparing for the first meeting, obviously doing quite a bit of background inform -- background reading. And I think there -- you know, it's -- I think the part of this that will be in some ways very difficult is the part that relates to public opinion, public acceptance, gauging that. So I think we're going to certainly try and figure out how we can get a better -- better handle on that. But I can say right now, there's not much out there.

Dr. Lin: And, as I remember, you've had a long standing interest in metrics on -- in this subject. Any advice that you can give us or papers that you can point us in the direction of would be very helpful.

Mr. Hoffman: Stay tuned. A student of mine and I have one coming out in communications of the ACM next month or the month after. I'll talk to you offline about it.

Dr. Lin: Fine.

Ms. Chemers: Great.

Ms. Sotto: Thank you. Mr. Palmer, do you have a question?

Mr. Palmer: Yes. Thank you for coming. As a security geek, another techy person, one of the challenges I run into all the time when I go to, as you are planning to, talk

about public -- talk to the public about their attitude about different things, I immediately run into, most of the time, a severe lack of understanding on the part of the public. I mean, my father, I always use him as an example, thinks cookies are the root of all evil and no matter what the benefit, even if it's IBM.com, he refuses to turn them on. How do you propose to at the same time query as well as make sure that they actually understand what you're asking when you talk to the public? It seems to me you need to lead with education then maybe an understanding test and then ask them what they think. How do you plan on doing that?

Ms. Chemers: I have no idea. I have no idea at this point. I mean, I think, and it will be obviously one of the issues that the committee will need to think about and determine, you know, their willingness to really -- to really grapple with this. I will say that the --the National Academy prides itself on the quality of what it produces. It wants -- it wants the information to be understandable. It presents it in many kinds of formats. We are hoping throughout the course of this study to kind of have a web page where we will invite comments from the public and perhaps we can work with you. But I think it's -- it is something that we're really, really going to need to think about. I mean, Herb has worked on a number of studies that - - where there was, you know, a lot of public -- worked on one on the privacy and the internet, and real con -- not privacy and the internet, on...

Dr. Lin: It was pornography.

Ms. Chemers: Yeah, pornography, pornography on the internet. And obviously -- big difference. And obviously there was a huge amount of interest in that study. The public has very, you know, very strong opinions and so I think it's something that we'll have to have to have some sensitivity to.

Dr. Lin: It's certainly the point that you make is very relevant, that often the public doesn't understand what it's afraid of. I mean, that's -- that's fundamentally your -- I think your point. We're not in a position to go off and poll the public and we don't conduct opinion polls or any of those things. We -- what we try to do is we try to understand polls that have been done already, get the -- get input from people to talk about the kinds of concerns they might have had about the validity of a poll and so on. Certainly the intellectual point that you're making is quite right and it's something that we would have to fold in to the study as it -- as it progresses. But I think that's the essence of it, that public doesn't understand things very well sometimes and you have to find a way of dealing with that in the public policy process.

Ms. Chemers: And at the same time, you know, there are huge differences as to -- depending up on your age in the public. That's what has really surprised me, when I described my study to my children, who are in their 20's, and their friends, I get a totally different reaction than when I describe the study to people who are in their 40's, 50's and

60's. Younger people kind of look at me and say well, what's the big deal. What's the big deal? So it's just such a totally different frame of reference. That's really kind of brought it home -- brought it home to me.

Ms. Sotto: Thank you. As is our custom on this committee, we recognize questions first from folks who have not yet asked questions. So I would apologize to Mr. Barquin, I'm not certain that we're going to get to you, but we might. We might. So first I'd like to recognize Ms. McNabb.

Ms. McNabb: Thank you, this looks to be very interesting. I don't know how people get appointed to this committee and I don't know if you have a role in choosing, so I don't know who I'm directing this to, but I would encourage whoever that is to consider including some known privacy advocates on the committee. There are those who are -- who are knowledgeable about technology issues. You could look to the Center for Democracy and Technology, to EFF, Electronic something, something...

Ms. Chemers: Frontier Foundation.

Ms. McNabb: Okay. I always think there's freedom in there. To Deirdre Mulligan at the Bolt Clinic, to somebody from the Carnegie Mellon Cyber Lab, there are a number of people that would be really useful and it doesn't look like you have that at this point.

Ms. Chemers: The names that were mentioned in the summary sheet were the original -- there were five members appointed to the -- my committee as kind of a planning group and among those is Fred Cate who was the -- worked on the Tapac report. There will be several people on the committee who are involved in the privacy -- involved in privacy issues. We also will bring in lots of people into the meetings to present information to the committee. So the privacy advocates really will have a real voice in this.

Dr. Lin: And also, part of their -- as part of the review process, that's another -- another part of it is that when we -- in peer review we take the theory usually that it's better to get the report shot at before it goes public rather than after and so we will distribute -- you can be sure that we will include privacy advocates among the reviewers.

Ms. McNabb: But not on the committee? Is that what you're saying?

Dr. Linn: No. No, I did not say that. I was just providing that as an additional place for where...

Ms. Chemers: Probably within two weeks the names will appear on...

Dr. Linn: On our website.

Ms. Chemers: ...on our website and it's open for public comment.

Ms. Sotto: I would ask if our panel minds staying for another five or seven minutes to continue asking. We'll cut the break a little bit short but there seems to be a lot of interest from this committee in your study. So if you wouldn't mind continuing that would be great. Mr. Wright.

Mr. Wright: My question's been answered.

Ms. Sotto: Terrific. Mr. Freeman?

MR. Freeman: Thank you. One thing you said struck me about the difference in age and perception, my -- I was struck when my six year old daughter asked me the other day what her email address is and I told her she has none and won't for a long time. But, so -- you mentioned, Dr. Lin, that you're not going to be doing your own polling but will be looking to polling already done and you may already know this, but probably one of the leading and most respected privacy pollers is Dr. Larry Poneman, who is ubiquitous and very busy polling on privacy issues. And I'd urge you to, if you haven't already gotten in touch with him, he might be a terrific person to come and talk to your group and help you understand his data.

Ms. Chemers: Thank you. His name surfaced very early on as someone who's been involved in this field and particularly around organizational work.

Ms. Sotto: Thank you. Mr. Barquin.

Mr. Barquin: Thank you Lisa and thank you. Having contributed to one of the national academies that are on the collection of statistical data, it really strikes me the importance of this difference between the uses of data for statistical versus administrative purposes. And at the heart of the study that you're trying to do and the whole issue of privacy dimensions of information is a term that I see nowhere in your summary. It's implicit in some of the things but not explicit, and vocabulary I think is important here. And that's the term screening. Screening with which we got bombarded, you know, from the very first day, and so many of the specific systems that are being put in place at Homeland Security and other agencies are in effect screening systems with purposes of using information to try to prevent terrorism, enhance administrative action with potential for harm on individuals. So the question is has this come up, are you focusing on this. Let me leave it there.

Ms. Chemers: Well, screening is a huge interest of the Department of Homeland Security and our project officer and that's -- and as I mentioned one of the -- one of the sort of groupings of technology is around deception detection, which is, in fact, these technologies are being used to screen. So while that word does not appear that, I'm sure it will appear elsewhere and it is considered clearly within the purview of the study.

Ms. Sotto: Thank you very much. This is clearly a study of great interest to this committee and I would again reiterate that we would be delighted to act as a resource to

you in any way that we can. If you are interested in having somebody from this committee liaison between this committee and your group we would be glad to do that as well. For members of the public, the summary description is outside on the table outside this room. We will take now a ten minute break. If you could please be back in your seats at 10:00. Mr. Alhadeff?

Mr. Alhadeff: Yeah. I realize that we were told that you had a bunch of questions for us which we didn't have an opportunity to let you give us, but perhaps you could submit them to us, because I think those questions would probably be informative for us.

Ms. Chemers: Many of the questions have been covered. I guess I did have one question and that was really for us to be able to identify more closely particular offices at DHS for whom this study would be of use. Obviously the privacy office is a -- that's pretty apparent, but I think our goal here is really to have this work be known by other offices who can also benefit from it and sometimes, at least for us, it is difficult to know who these people are. For our first meeting I kind of rounded up, you know, a group of suspects for the first meeting, but it something that you could definitely be of help, helping us identify. I would also like to offer to come back at one of your future meetings and kind of give you a status report and kind of how we're approaching it.

Ms. Sotto: We will certainly take you up on that offer and very much appreciate it. Becky, if you could assist in getting that information. Yes?

Dr. Lin: Just comment to all panel members here, feel free to contact either Betty or me with any questions that you have about the study, any input that you want -- that you think is important for us to know, and of course, for any members of the public out here, please feel free to do the same thing. We really intend to cut as wide a swath in terms of getting public input on this. We recognize the losing nature of hiding this study behind closed doors. So please, anybody with any comments, let us know.

Mr. Chemers: Our email is simple, it's either b __ c __ h __ e __ m __ e __ r __ s __ @ __ n __ a __ s __ . __ e __ d __ u __ or h __ l __ i __ n __ @ __ n __ a __ s __ . __ e __ d __ u __ .

Ms. Sotto: Is there a website? You had mentioned that...

Dr. Lin: There will be.

Ms. Sotto: ...the names will be posted. Okay. Maybe you could let this committee know and we'll make sure that that information gets out. I think a continuing dialogue would be very useful and we certainly offer to help in any way we can. Thank you very much. 10:00 please, back in this room. (Break)

Ms. Sotto: Thank you very much for our panel for taking their seats and being ready on time when the committee is not quite ready on time. Our next panel will be

focusing on building an information sharing environment. Our first speaker on the panel is Dr. Carter Morris. Dr. Morris is the Director of Information Sharing and Knowledge Management for the Officer of Intelligence and Analysis at the Department of Homeland Security. Previously, Dr. Morris served as the Deputy Assistant Director of Central Intelligence for Collection where he helped coordinate all intelligence community collection files. Dr. Morris BUILDING IN INFORMATION SHARING ENVIRONMENT:

Dr. CARTER MORRIS, DIRECTOR, INFORMATION SHARING & KNOWLEDGE MANAGEMENT, DHS INTELLIGENCE AND ANALYSIS, ACCOMPANIED BY: MR. AL MARTINEZ-FONTS, ASSISTANT SECRETARY, DHS PRIVATE SECTOR OFFICE, MR. CHET LUNNER, ACTING DIRECTOR, DHS OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION

Dr. Morris: Thank you very much. I welcome the opportunity to talk. I hope we will make this very short as far as my comments and let you ask questions as you see fit. I am from the Office of Intelligence and Analysis. I work for the Assistant Secretary for Intelligence and Analysis. We clearly are charged with providing the Secretary with his intelligence information, hopefully, in a way that leads to actions and decisions appropriately. The Assistant Secretary for Intelligence and Analysis is also the Chief Intelligence Officer for DHS and as such he oversees the intelligence enterprise within DHS which include the intelligence components of the other components of DHS and a lot of those having to do with law enforcement and, therefore, we get into the case of where we're bringing intelligence and law enforcement data together within the intelligence enterprise.

One of the things we've established is a Homeland Security Intelligence Council that brings together these organizations across DHS is a way that we hopefully we can coordinate that. As I said, we are the Secretary's prime intelligence organization. As such, we do a number of different things for him. We try to provide warning. We try to research issues and to basically discover threats out of where there might not be threats, and I mean real ones. We analyze information, we pour through that. We try to provide in-depth analysis on groups and types of potential threats and we try to feed that definitely into the preparedness situation so that people will know what to prepare for out there. In addition to providing the Secretary his information, one of the main things that we have is to build an intelligence environment with state, local, tribal, and the private sector. Clearly, one of the great responsibilities that DHS has is to pull the entire country into a Homeland Security posture. And one of our jobs is to make sure that we build an information sharing environment into those other domains such that we can freely move information back and forth with the state -- with the states, localities, et cetera, and with the private sector which we'll hear more about. That's a real challenge in that area when it gets into the privacy domain because anything that comes back into us

through that domain is almost exclusively going to be U. S. person information. And the question is how do we handle that appropriately, how do we integrate that with the foreign intelligence information that we have, and how do we ensure that we keep the parts together appropriately in handling that kind of -- and as I say quite often, how do we handle it in an auditable manner that we know where things are and we know where to find them.

As I said, one of the other key issues is dealing with the components within DHS, as part of that flowing information from the law enforcement parts. Quite often I see come through information that contains U. S. person data in it and how do we fully protect that, how do we ensure that we can use it, and how do we ensure that we purge it according the rules and regulations are key aspects of what we're trying to do.

When we try to do the intelligence mission with DHS one thing that intelligence is forced with was dealing with very many different types of information, and coming out of the intelligence community, one of those is that we must deal with multi-levels of security, on classified information, secret information, top secret information. Under my desk I have a computer for each of those. I have to handle each network separately. We do not have connectivity between them. We can't electronically move information from one level to another.

In addition to all of those, what I'd call federal classification programs, we also have to deal with many other types of what we'll call sensitive and unclassified information. SBU. And there it gets into law enforcement. The state has a lot of that kind of information. You can name -- I think we go through certainly tens if not hundreds of different types of designations of sensitive but unclassified information. Part of our challenge is to appropriately handle all of that and move information back and forth between the various levels.

When people ask me what are one of the challenges in sharing information, the one thing I identify is figure out a way that I can effectively move information between security levels, effectively. And I'm not just talking about technology I'm also talking about processes by which we ensure that we do it appropriately.

Clearly, handling U.S. person data within that is a clear issue for us. We need to make sure we go by the rules. We need to make sure also that we can use the effectively in our intelligence business, sharing with state and locals.

One of the things that, you know, if you read the legislation that created us and if you read the intelligence reform legislation, one of the things it says is we want you to get information out to state, locals, and private sector very effectively. We want you to make that a part of the way we do business in the Homeland Security business. And they say in general we want you to declassify as much information as you can. Well, we try to do

that but coming out of the intelligence community, the intelligence community keeps saying sources and methods, sources and methods, you got to protect sources and methods which is clearly we do.

And what we are finding more and more of is that we can share a lot of information at the unclassified level but when it gets down to taking, for people to make decisions, and quite often in our business what we're doing is providing information to state, locals, tribes, and even private sector where they have to make real decisions. They have to make resource decisions, they have to make decisions that will inconvenience people. To make those kind of decisions, we have to ensure that they have all the information that's there. Frankly, they don't necessarily want to take our word for it. And to do that it is driving, in my opinion, us to share more and more classified information. Now, we can do that. We have methods and processes to ensure that we can do that. However, it also means that we've got to clear more people so more people are going to have access to that information. And the more people who have access to information, the more chances it is to get out into an unclassified world, it's more chances to compromise sources and methods and make it harder for us to get information the next time, so a real challenge for us.

Getting information into intelligence and analysis. That's where we clearly get into the U. S. person data. This is where we've got to really make sure we handle it. One of the systems that we're trying to develop now is a much more robust system of sharing unclassified information, intelligence information, with state and locals in a very focused way between us and DHS intelligence and the various other analytical activities that are going out all over the country here. When we start looking at the issue of us posting information for them and us sending them information, everybody's pretty comfortable with that but when you talk about them sending information back to us and now what do we do with this, us big, bad guys in the intelligence community, and how do we appropriately handle that then people get more concerned and that's where we have to address a lot of the issues that I'm sure that you have been looking at during that time. And one of the main issues that we have in all of this information sharing is to ensure that we are really looking at information appropriately.

One of the big problems we have these days is information getting out and it becoming very alarmist. And as I've said to people, in the four months that I've been at DHS, we seem to have spent more time in intelligence and analysis telling people there wasn't a threat than we are telling people there is a threat. So you have to look at information sharing within that context of what reaction are you getting with the information you send out and is that the appropriate reaction to the information you send out?

I think we all have heard about the New York subway cases and the Baltimore tunnel cases. These were cases where local and state governments took actions, very, very appropriate actions, when in the end the level that we could certify that there was really a threat was questionable. And that's not a criticism of any action that was taken because they have to make those decisions and they're very hard. But we have to in a sense be effective in getting the information out.

Let me just summarize then for you just a couple of things. One, we're establishing an intelligence domain within DHS. Two, we're making sure that all the components in DHS share information effectively. Three, we're connecting the intelligence community to state, local, tribal, and private sector. Four, we're creating an information sharing environment with them that allows, for instance, analysis to go on, not only in the federal government but in those other places. And, five, we're working very hard to make sure that we manage all the information, including information that privacy and civil rights gets concerned about, in a very professional manner and in accordance with all the rules and regulations, although I'm not sure we understand what they are sometimes. And let's stop at that.

Ms. Sotto: Thank you very much. Questions, please. Mr. Hoffman.

Mr. D. Hoffman: Thank you, Director Morris. And this question may be unfair and tell me if it is. I'm just trying to get some information. I'm looking at the memorandum that came from the White House for the heads of executive departments and agencies that was issued I believe on December 16, 2005, for governance and requirements in support of the information sharing environment. And in section two of that it has a requirement for information sharing guidelines to be published within 90 days and then within the 90 days after that, if I'm reading this correctly, for the Department of Homeland Security and the Attorney General to jointly disseminate those guidelines and standards out to state and local and tribal governments. And I'm just wondering if you could comment. I may be misunderstanding this, first, and you could help me with that if I am, and if I'm not could you tell us what the status of those are and where progress is and who's playing a part in the development of those?

Dr. Morris: That particular one I think the first thing it says is to develop the standards and that's the case. I get the honor of being the DHS representative to the information sharing council and that's the information sharing program managers overseeing a lot of those activities. The standards that they're talking about have been developed primarily over the last at least three or four years that the intelligence community has been working with various other departments in trying to come together with some standards for how we handle information, meta data standards, how we do those kind of things. They were actually handed out last week from the DNI's office or particularly from the ICCIO's office who had been the coordinator of those activities.

They are now being reviewed by all of the departments that are part of the information sharing environment to essentially see if we agree or if we have problems with it.

I was just reading this morning somebody reading and saying, I'm not sure where that came from, but they are now in Federal review. After that period of 90 days which I believe is supposedly up about the middle of this month, they will be turned over to Justice and Homeland Security because we are the ones that have the interface responsibilities to state, local, tribal, and private sector and we will be sharing those with them to get response.

What we're trying to do is to get data into a way that, one, is shareable but it's also researchable, that we can easily use tools to get through the data that it comes in and some of the formats and so on. We cannot dictate standards to state and locals. We can only advise. And so if we -- as much as we can we will try to get them into that kind of mode. Justice has had some very good results within the law enforcement community into bringing common standards into that. This is an effort to try to extend that into a more broader Homeland Security information sharing counter-terrorism type of business.

Mr. D. Hoffman: Thank you. That's very helpful. Two follow-up questions that are very quick. One, is the Department of Homeland Security Privacy Office involved in that review of the standards? And, second, is there a point at which those standards would be appropriate to be shared with this Committee, specifically with the Data Sharing and Usage subcommittee so that we could take a look at them so they would help and form our analysis?

Dr. Morris: I hope the Privacy Office is involved in that. I don't know any reason why they shouldn't be. We're now running through the reviews. We've used kind of standard procedures. We ran it through the DHS CIO's office to make sure that those kind of coordinations are getting done. I will make sure that's happened. I see no reason why those standards couldn't be shared with anybody, personally.

Ms. Sotto: Becky, could you follow-up on that, please? Becky: Thank you. Joe Leo.

Mr. Leo: Yes, I have two observations, two points, or maybe one's an observation. The first one is the issue of coordination and clearances. Getting with your state and local partners, I'm from the private sector. I realize that there's over a two-year backlog in getting security clearances for the contracting community that work directly for the Department of Defense or civilian entities like the Department of Homeland Security so I'm wondering what can be done about that. There was an executive order issued recently but there still seems to be muddling through in the administration of that order about the OPM doing more centralized clearance processes. And then my second point, there's a connection here, I'm not exactly how or exactly if there's a clearance problem is the just seems to me from an outsider a little of a culture clash between the intelligence

community about your statement about protecting sources and methods and the law enforcement community that wants to go out and grab your source or to lead to an actionable arrest or something else. And I'm wondering how you wrestle with that seemingly clash paradigm between law enforcement and intelligence in the culture part and then, of course, what your observations are on the clearances.

Dr. Morris: On the clearances the private sector office has some information, I'll let him talk to you about it, but I think the clearance issue is a big one and it does take time and it's historical and we're trying to clear more and more people up.

I know that Congress has beat on the intelligence community unmercifully about getting more resources against it so I think there are efforts to do that. I know DHS has worked hard on trying to accelerate the processes as best we can but I also know that the numbers that are coming into us in intelligence and analysis for wanting to clear state and local people are going up -- the more we interact the more we create an environment the more people they want cleared so it's an accelerating problem in that sense.

But let me go to -- let me finish on the issue of conflict between law enforcement and intelligence. Very different environments, but let me say from the point of view of what we are trying to do in DHS in working with our law enforcement components and with intelligence and what we're trying to reach to state and locals and work in that environment, I really think that's a workable issue. I don't see us running into real problems. I think there's a pretty good working relationship between it. The issue you talked about, the intelligence community has had for a very long time with the military, you know, we have sources and methods and they want to go bomb them. And so that's been a historical contention point of how do you balance between leaving the source there and taking them out, but I really don't think that's a big issue for us. I think we have pretty good relationships now and we try to work through those issues hand in hand as best we can.

Mr. Martinez-Fonts: Joe, good morning. Good to see you. Just very quickly, our office has been working with the critical infrastructure group under Bob Stephen, Jim Caverly, that who group and if you are, and this may be the caveat, you know, if you're in critical infrastructure we've been getting clearances in about six months. Admiral Jim Plehal from my office has been working on that again with Jim Caverly's group and Chet was also saying that they've been -- had some success.

Mr. Lunner: Yes, in the state and local area as opposed to the private sector the Homeland Security advisors and those sorts of people get their clearances quicker than -- I mean, it's longer than people like but it's a lot less than two years and one of the ways that we've managed to speed up the process a bit is to enter a compact where the different departments in the federal government recognize each other's clearances so we don't have to redo yours if you've got one from the FBI.

Dr. Morris: Relative to that, one of the things that we set up a group actually a couple of months ago that's looking at all of these kind of issues. We've formed a group with us and with Justice and we've brought the whole community in on how do we move the classified domain out into the state and local environments? So we have an active, ongoing effort looking at exactly that right now.

Ms. Sotto: Mr. Herath.

Mr. Herath: Thank you. I think Joe hit on part of my question and David sort of hit on part of my question, but by having been involved in the private sector in trying to build what in essence is a large data warehouse, right, how do you secure and how do you govern this thing because you're going to have to have separate visibility rules and access rules. Some people are going to be able to access some, some other portions. You're going to have to have the ability to take in data from local and state, tribal sources that may or may not be sophisticated so you're going to have data integrity issues. What is the governance model? Do you have a governance model architected yet? You know, this is like the big glowing brain, right.

Dr. Morris: Do I have the model yet? I couldn't say I have a perfect one. I think what you have certainly within our organization, you have a conscientious work force that's trying to do that. One of the things that I have done since I came in and actually at my boss' direction was a pusher on this, we have right now an intelligence domain information architecture study underway to look at exactly those issues.

It is a concern of mine since I've been there as to whether we have the right architecture to do the kind of things that you're talking about, but I have -- the first part of that is due by the end of the month, as I told my project lead on this 25 days from yesterday, is our first cut at that. I think this is one that is going to identify for us the needs to do that. We have within our own organization to build the data structures that we can pull in and do effectively. We within DHS as a whole how do we tie all the components and intelligence together effectively and deal with all that? I can't say we have all the answers. I don't think anybody does. But I do know that we are very consciously working on it and we're trying to build the architectures.

You're talking about dealing in databases, one of the challenges that we're taking on as a community, as part of the information sharing environment community right, is what we would call the terrorist nexus and how do we ensure that we can basically search out information about that. In general, and I won't get into the details, but the law basically allows us to look at any data to which we can make a terrorism connection or a person or terrorism connection. And they have that right and I think other organizations within the federal government have a right to look at data if there's an established connection to terrorism or a person associated with it.

What we would like to be able to do is ensure that we take our database of terrorist related people and run it against databases in general to ensure that we only get back information where that connection is made. That is, how good a match does this person have to be here to the person in the database in order for me to pull that record back in legally? If I'm pulling back in records that are not terrorism connected then that's, may not be right, but if I'm pulling back from your vast database only those informations that people that I already have a terrorist connection to then that's legal. So figuring out how to do that is a project that we're taking on as a community right now of understanding how we could effectively do that kind of connections.

And I think we all agree that in the information sharing council that this is a project that we wanted to take on. How do we effectively do that? And in some sense that would isolate us from the information because it would automatically only pull back the information for which we identified a real need for. Do we know exactly how to do that now? No. But we know it's a problem.

Ms. Sotto: Ms. Lemmey.

Ms. Lemmey: As I mentioned in an earlier question, I also sit on the Markle task force so a lot of this discussion is very common for me and one of the -- there are two things I come up right away that I have a question on. One, is that we found in that work that in a lot of ways DHS has the most privacy sensitive information almost of any organization, and in the effort to begin the information sharing process, a lot of noise is being made about actually sharing more data when what we found is that it may be best to leave the information where it is and perhaps do the analysis here and not have that information transported over because it's between those seams and at the point of transport that more of the privacy issues come up.

And I know that there was a lot of discussion about how that was feasible, what was possible, and the technology front to allow the analysis where the data resided with its steward as opposed to transporting that data and much in the effort to do this on blind analysis for finding terrorist related information. I'm wondering on that question what progress has been made and is that what's happening or is the data being still sent in sort of a more comprehensive perspective? And on the issue that you just brought up about matching against databases, when I've done analysis on that previously, we found out that there can be a high degree of correlation with not necessarily appropriate people and that some percentage is where you need to have a cut off and I'm wondering if you guys have gone into the determination on that and what the process for doing that is.

Dr. Morris: On the last question, that's exactly what we want to look at in this study that we're doing is exactly what you just brought up. How good does the match have to be in order for us to be able to -- have a defendable criteria, and I think that's the bottom line. We could justify to you or anybody else that we have a defendable criteria.

So that's exactly the problem we want to look at. On the other issue of where we do the analysis on the data, I think that's a question that's still open. I think in general if you look at kind of the philosophy that's behind the information sharing environment it is a philosophy that we allow people to see the information themselves. I didn't say it was right but I think that's kind of it. It's like everybody can see everything they're entitled to. But the issue of whether we analyze the data in place or whether we allow somebody remotely to get into that database and do their own searches and to pull the data is still an open question. I don't think we've decided in some sense.

I think the issue that I see is I still see the pressures are the ones that say I want access to your database, whomever that is. I think that other pressure -- the question of I need information out of our database, I will let you search it out and give it to me, seems to be the secondary answer at the moment. Now, we continue to ask about okay is that the right way to do it but I think that's a question that's still unresolved basically.

Ms. Lemmey: So let me just follow up on that for a second. What we found is that the issue of transport, once the data has been transported to other organizations it's certainly under the current technology much more difficult to track. It's not as if we're sending meta data contracts with and once it's gone it's gone and some of those folks may not be high correlation matches or maybe part of them are comprehensive database so a lot of the argument would suggest for at least both privacy protection and the vitality of the data that it stay within its stewards. Are there people arguing against that for reasons that we should be aware of or is that still under consideration?

Dr. Morris: I don't know if anybody's arguing specifically on the merits that you were just discussing. I think the issue becomes in general that we hold certain organizations responsible for having their fingers on the data and people feel that pressure to do that and so they want their access to the data. I think there are legitimate issues having to do with how well can you analyze data -- there's a feeling that you can analyze data if you have direct access to it more readily. All right?

I think there's an inherent feeling that that's there and so I think people are trying to work against that. Now, having said that, there are many databases that we run into that are what would I call -- not well-structured, all right? And I've been told by many organizations that say if you try to go search my database without being an expert on this database your chances of using it well is not very good. And I believe that, I very much believe that. So we're caught between those two forces. I don't think there's a -- I don't think we've decided, I mean, I think there's still pressures. People say, in fact people out of my own office say, we need access to that database. Being my job, I got back and say okay tell me what you need exactly access to and what's the right way to get that? And that's one of the questions that we continue to present. I think we're still working through

it to be honest. I don't think there's an answer one way or the other. I think we're still working through it.

Ms. Lemmey: So you'd be open to us participating in maybe architectural solutions that enhance the approach to privacy?

Dr. Morris: Absolutely. I think we continue to look at that, absolutely.

Ms. Sotto: Mr. L. Hoffman, you may have the last question, please.

Mr. L. Hoffman: Thank you, Madam Chairman. Dr. Morris, I was interested in your discussion about the promoting data sharing and in particular the answer to Mr. Herath's question on the governance model because I'm interested in what Ms. Lemmey was getting at also, in essence the accountability issues. You're working on the study, the intelligence domain information architecture study, is that -- are you planning to share or maybe you already have I don't know, with the Privacy Office?

Dr. Morris: I don't think that's been the emphasis of what we've done. At the point there's no reason we couldn't do that. It just hasn't come up because we're still -- we certainly are as we're looking at how we handle data taking into consideration the privacy rules as we know them. I don't know that we have specifically engaged the privacy office on it but I don't have a problem with doing that.

Mr. Hoffman: One follow-up, if you don't have a problem doing that, the reason I asked that is because we've had testimony in the past in earlier hearings from other people that research in both the Homeland Security and other departments as well sometimes treat privacy as too hot to handle, all the research doesn't get done, doesn't get funded and then later you have things getting sandbagged like programs get half way, they get started, the public gets wind of it, and they get killed or driven underground and become less effective sometimes. I would -- I wish if you could you would share this study, these efforts, with the privacy office in an effort to prevent this because I think otherwise it -- we have too many examples of not examining privacy up front early in the past and programs suffering in the future.

Dr. Morris: I will go back and tell my team lead to do that. I have no problem with that. Let me say though that one of the things that I have spoken to my team lead about very strongly and what they've been doing is my concern of whether we are handling data within our systems with privacy concerns and legalities take into account. So they are very aware that that what we're doing here as part of this architecture has to take that into account, but I will make sure they go talk to the privacy office.

Ms. Sotto: I would echo Lance's suggestion and repeat what the Secretary said this morning. He said, we are aiming to build into the sinews a respect for privacy and a thoughtful approach to privacy, so I think that that building privacy in from the start of any new technology program or matrix is really -- would be most effective for you so that

nothing gets torpedoed later on. I welcome our next speaker, Assistant Secretary Martinez-Fonts. Mr. Martinez-Fonts was appointed to head the DHS private sector office on November 27th of 2005. For the two years prior to his appointment, Mr. Martinez-Fonts served as special assistant to the Secretary for private sector. As Assistant Secretary, Mr. Martinez-Fonts is charged with providing America's private sector with a direct line of communications to the department.

Mr. Martinez-Fonts retired in 2002 as Chairman and Chief Executive Officer of J. P. Morgan/Chase Bank in El Paso, Texas after a 30-year career. Thank you and welcome.

Mr. Martinez-Fonts: Madam Chair, thank you very much and it's an honor and a pleasure to be here with you today. I thought I would start with I'm going to call it my standard spiel on my office because people often wonder what it is that the private sector office does. It is a very unique organization not just within the Department of Homeland Security but within the federal government as a whole. And when I talk about what it is that the private sector office does I talk about four things that we do. Interestingly enough one of them is very apropos to what we're going to talk about today.

Number one, we are an advocate for the private sector, so we're out there. This doesn't have to do with selling products but on strategic issues we're advocating on behalf of the private sector.

Secondly, we share. And what we share is information and best practices, and I'm going to come back and really what I will focus on is that information sharing side of it.

The third thing that we do is we help promote public/private partnerships. Now, while we have no corner on the market within the Department of Homeland Security on public/private partnerships, we clearly try to link up and make sure to a great degree, call them Chet's world or Chet's customers in the state and local and the private sector are linked as best they can.

And, finally, I look at the economic consequences that impact the Department of Homeland Security as well as the private sector. So we look at those from two sides. We look at them on the micro side. A very easy example would be if we decided to put seals on containers and today the seals are lead seals that get numbers stamped on them and they cost fifty cents, if we decided to put a $500 seal that has GPS and RFID, et cetera, your sneakers from Taiwan are going to cost a lot more and so what is the impact on that on business. We also have been doing a lot of work on macro-economic, including most recently having to do with not just exercises but with Katrina and very most, most recently in connection with pandemic flu and what the impacts of that may be.

So basically those are the four things that we do. We advocate, we share, we do public/private partnerships, we look at economic consequences. When we look at the sharing of information which is the area that I've been asked to talk about, I thought it

would be very important for me to share with you what it is that we do when it comes for information sharing.

In effect, it is Carter Morris' group, Director Allen that prepares that information. We do not prepare information that gets to be shared. But our goal has been, again, somewhat of a two-pronged attack. On one side we have been pushing them to get as much information where one of the people that he somewhat complained about probably were trying to get them as much information declassified, unclassified, so that information can be shared as broadly as possible. We do not deal with secret -- even though I and people in my office have secret, top secret, SCI clearances and the like, we do not deal with that information. We do not have the way, the mechanical way of passing it so we are constantly trying to work towards the tear line, we're trying to work towards the information that can be declassified, unclassified. At the same time we are working as I mentioned in answer to Joe Leo's question, we're trying to get people that I will say need to, deserve to, have to be -- get that secret or top secret clearance, we're working to get those expedited.

To give you a little further information on this side, I believe that what the private sector wants at the end of the day is that they're merely looking for, and I say merely as if it were something easy, but timely, accurate, and actionable information. And I will focus on that actionable information and I will talk about it again to a certain degree. I won't say in contrast to what Carter talked about but since I had the opportunity to listen to what he said, I'll let you know that I think we have no conflicts in what we're trying to do.

But that at the end of the day I'll give you the example of August 1st of 2004 when there was a threat against financial organizations, primarily specifically named were Prudential in New Jersey, Newark, CitiGroup in New York, the World Bank and IMF here in Washington, D. C. We were able to reach out to those individuals and share with them the information through the state and local group we were able to share with the local police, et cetera. At the end of the day when I receive calls from some of those people because they oftentimes after they get sort of the official message they call my office and say hey the answer was not I want the sources and the methods, I want to find out who it was, they wanted to know what do I do. Do I need to put the Jersey barriers in front of my building? Do I need to check -- how do I check for ID's? What are we looking for? Are we looking for a guy who may have a bomb in his shoe or is it going to be in a briefcase? What should we be alerted for?

So at the end of the day I am a big believer that as we work through information sharing types of issues, what the private sector is trying to do is get that actionable information that is obviously on a timely basis as well as accurate.

I'd like to just talk for a moment also about the cultures that are involved. Clearly, whether it's the intelligence culture or the state and local culture, I conveniently have

them on both sides and I represent the private sector culture. You know, we have different ways of handling this information and it means different things to different people.

Again, Carter talked about the fact that we spend an awful lot of time trying to dissuade people from putting or telling them that this information that was put out there is either not credible or not to worry about it. That causes great consternation with the private sector. I am almost hesitant to use a name in particular but we have heard a lot from them.

You know, when we put out things that say theme parks are going to be, you know, are in some sort of stream that we've learned or, you know, banks are in a stream of information and so on we tend to want to say a name and we try to say something. Well, that creates a great deal of problem for that individual company. They don't want -- if they have been named, they would like and they should and by the way I would say that they do get a phone call whether it's from our office or from the intelligence side of the shop letting them know specifically what it is they need to know.

So you need to be aware of the fact that at the end of the day we could literally be damaging the trademark, the value, the corporate name, the good name of a company. When we talk about information sharing, I've talked about what it is that the private sector is looking for. I believe what the government is looking for is, is we are looking at vulnerability information and we are looking at incident information. We're trying to find out, we're trying to get situational awareness of what's going on, and the private sector, while they are willing to share certain of this information, they've been reticent about providing some of this and that it could potentially compromise their situation.

Again, I'm going to speak very personally, I believe litigation is an issue that the private sector is extremely concerned about. They're very concerned about regulation and, of course, they're very concerned about competitive information that may be shared outside. What the private sector, and this doesn't just have to do with information sharing, but I believe what the private sector is looking for from the government are some kind of standards, some kind of what should I do, some kind of best practices, again, those are at different levels, and in exchange for that if we want to call it the private sector is looking to be relieved of some liability. The private sector wants to know if I do the right thing, if I secure my facilities, if I share this information with you and what you share back with me allows to do something, I want to make sure now I'm not going to get sued down the line. We haven't been able to really give them that.

I'd like to just close since the idea was just to talk for a few minutes on PCII, protected critical information, and the fact that we have protection of critical infrastructure information. I saw some people they use three words to it say four letters, but at the end of the day that is a program that has not met with a tremendously great

success. We are exempted from FOIA, we're exempted from state sunshine laws. The final regulation ought to be out soon but there has been a very slow start. And, again, I go back to very much of those same reasons that people are concerned. If I am a company and I submit this information, could it in a civil case, could that information be somehow subpoenaed and I have to release that under a civil case even though again we believe that we're protected from that but it's never been tested and therefore people are concerned.

What kind of regulatory, again I'll use the word punishment, you know, if another agency finds out I have a hole in my fence and that's what creating the problem, what could they come back and hit me with? What might my competitors do to take advantage of it, et cetera? And so with that I'll just close and open it up for questions. Thank you.

Ms. Sotto: Thank you very much. I'd like to actually ask a question. Do your private companies share personally identifiable information with you, under what circumstances, and would it be without a subpoena, and do you ask without a subpoena?

Mr. Martinez-Fonts: When you say personally identifiable information, for example, as a customer the organization or.....

Ms. Sotto: Yes. Both customers and employees, for example, of the organization.

Mr. Martinez-Fonts: The answer is no we have never asked for that information out of our office nor has anybody shared that information. Interesting when you talk about their employees. One of the requests that we have had on a fairly wide-scale basis is for companies asking us to do background checks on their employees which we can't do but that doesn't stop them from asking.

Ms. Sotto: Thank you very much. Ramon.

Mr. Barquin: I'm glad you asked that question, Lisa, because I was going to ask then how do you reconcile requesting information say from a airline in terms of its passengers or its crew -- however, I wanted to put that into the, into my specific question, which was it's tied to redress and you spoke of the fact the private sector normally wants something in exchange for providing the information, and because this committee has to deal with data integrity, we think it also makes a lot of good sense to find ways of having that feedback loop to be correcting and constantly improving the intelligence databases and the supporting databases that you'll need to do your job.

Mr. Martinez-Fonts: When I answered the question about “we” I was referring specifically to my office, to the private sector office. I was not referring to the department as a whole. In the example, Ramon, that you just used we have, for example, the TSA requesting this information or, you know, CBP as someone is coming across the border and the like, to talk about, if your question specifically is about the redress, I think that there have been a number of programs that have been put in to make sure that that is both

expedited, because I think one of the complaints was that okay I can get my name off but it's taking me so long and I'm traveling every week, that that's been taken care of.

And you may be aware under the Rice/Chertoff initiative that Secretary Rice and Chertoff put out just a month and a half or so ago that one of the goals in that is to create a redress mechanism that would be able to help anyone who is turned down for a visa and all that type of information. So I think it's -- and by the way, may not just be my personal experience but again I get a lot of people calling my office saying hey my executive vice-president is such and such is on this list or he's been stopped and whatever we've been able to get fairly quick resolution on those issues.

Ms. Sotto: Thank you. Mr. Alhadeff.

Mr. Alhadeff: Thank you. It's -- and this question is actually directed just to the operation of your office, because it sounds like in a large manner you're in charge of kind of an information decimation of non-classified information and as broad a range of that non-classified information as you can get and as actionable a set of that information as you can get. And you talked about how you do some of that but I was waiting to hear about perhaps how there is coordination with other groups, for instance, with CERTs and ISACs where some of this information sharing is going on and some of this decimation, or in the case of avian flu or a HHS, that might be doing some of this and, you know, how is there interaction with the disaster preparedness schemes that companies are using?

Mr. Martinez-Fonts: Very good question, and I apologize that I didn't actually discuss the whole idea whether it's CERTs or ISACs or the sector coordinating councils. As you know, over in the now the preparedness director under George Foresman, one of the groups that I'd say really pretty much transferred from the pre-second stage review Department of Homeland Security was Bob Stephan's infrastructure protection group. His world has Jim Caverly who does the sector coordinating councils and we are involved very closely with Jim. I mean, we're connected at the hip in terms of putting out information, reviewing things that he puts out, working with the ISACs, working with the sector coordinating councils so very, very closely connected. The difference for those of you that are not familiar with the critical infrastructure versus my office, my office is looking everything private sector on a strategic basis. The infrastructure protection group is looking at critical infrastructure which are the 17 defined critical infrastructure and key resources and making sure, if I could also move into the avian flu situation, that we are working very closely. I'm on the pandemic flu tour with Secretary Leavitt, as is Chet. There are four of us from the department that have been traveling around to 60 cities, or will have gone to 60 cities by the time we're done. But on the critical infrastructure side and our message in working by the way very closely with HHS is we want to make sure that the electricity stays on so that when the healthcare people need to put people in the

hospitals or people need to go to the hospitals that all of that is there. So the answer is we work very, very closely with all of the critical infrastructure side of the shop.

I would say we work -- my office is very much organized to serve, you know, science and technology, the preparedness director, intelligence and so on so that I have people that work for me and they work in my shop but they are there at all of those meetings and all of those to make sure we're coordinating. We often become a vehicle as you said to share information and sometimes it is purely, for instance, during the hurricanes our office held at one point it was twice a week and then later on reduced to once a week a meeting for just getting people as a place for people to come together and coordinate and share information about how to get diapers into the such and such a center, you know.

Ms. Sotto: Thank you. If there are no further questions, we'll move to our next speaker on the panel, Mr. Chet Lunner. Mr. Lunner is Acting Director of State and Local Government Coordination for the department. He was appointed in November of 2005. His office located within the DHS Preparedness Directorate and Mr. Lunner is responsible for coordinating the department's pandemic preparation and response issues with respect to the DHS chief medical officer. Previously Mr. Lunner was the Assistant Administrator of the Transportation Security Administration for Maritime and Land Security overseeing TSA's development of security policy and practices for the non-aviation sectors of the National Transportation System.

And I will just preface your remarks by telling you that we are working, we're at the very preliminary stages of working on a paper on national emergencies and data sharing within that environment, specifically using Katrina as an example. Thank you very much for joining us.

Mr. Lunner: Thank you and thank for the invitation. This is -- with apologies to Dr. Morris who's heard me screaming this from the roof-tops for months now, it gives me a chance to repeat my stump speech on this very topic. As you mentioned, my office is in the preparedness directorate which just about the only difference between what Assistant Secretary Martinez-Fonts just described as his roles in the private sector. If you just substitute the words state and local government for private sector, that's exactly what we do with Homeland Security advisors, the governors, the emergency managers, police chiefs, fire chiefs. We are their advocate in the department at the department level.

We advocate for their resources, we facilitate, we don't -- we take the information that Carter talked about and facilitate getting it out to them in a timely basis. We don't collect or manage it. And we maintain that relationship generally across the board at the corporate level for the state, local, tribal, and territorial officials. I'm also serving with Dr. Morris on the DHS committee that's attached to the DNI's effort for the information

sharing environments so I have a long-standing interest in this from in my days at TSA and before.

I'd like to start this conversation with the way I always start these meetings on these topics, usually with intelligence people in the room, is that we have to adopt a common lexicon before we go much further in the discussion because I've found that often the definitions of what we're talking about in the different customer basis and the different data that we're trying to use gets confusing.

And my -- I noticed in the President's National Strategy for Homeland Security a paragraph jumped out at me where he said that we must build a system of systems that can provide the right information to the right people at all times. I think there's a variety of information and I always like to make the distinction between intelligence and information. A lot of the discussion seems to go along the lines of intelligence and traditional data that's in that realm because that's most of the people handling it are from the IC. In the new post-9/11 environment, however, what we're looking for is more like what Al Martinez-Fonts was just describing, actionable, timely information. I make the distinction between intelligence and information because I think that there's a lot of information that's available to us that we already own that we don't need to go out and collect more of that we can develop and make more useful to our state and local stakeholders.

I'd also like to follow-up on the point that was made earlier about the difference between law enforcement information and traditional intelligence information. There's yet another iteration of that in my world which is the operators that are neither law enforcement nor intelligence practitioners. They're subway drivers or, you know, the Homeland Security advisor who's neither in any of those categories but straddles both of them somehow. So there's this third line of information that's sort of part LEO and part intel that we have to develop that's useful, that's not at all classified. I take sort of a reverse view of what's been talked about earlier today on the tear line issue.

I don't think that we need to declassify information more, although that's one thing we need to do, I think that we need to not classify it to begin with and look at this pool of information that we've got that's useful at a -- I don't want to say a lower level but it's certainly a lower level of classification that's closer to the boots on the ground. They don't really need to know sources, methods, intricate, complex relationships back to, you know, tracing this information back to Baghdad. They don't really have a need for that.

I'll give you an example. In my neighborhood not long ago it was -- I was out walking the dog when I heard a scream in the neighborhood and suddenly the police patrol person showed up and I asked her, you know, what was up. And she said they were looking for a man who was, you know, 5'7" and wearing a yellow jacket or something who had started to attack a runner, a jogger. Now, it struck me later that that's

the kind the information that my operators are looking for. I don't care what the man's name is. I don't care where he was born, what his blood type is or what his affiliations is, I'm looking for a guy in a yellow jacket that may do harm to my system in some time period that's been identified. That sort of information I think, activity, not individuals, but activity is often open source. It's almost entirely open source in my experience but it's something that has not been produced as much I think partially because it's in an abundance of caution we tend to put everything behind the classification shield until we sort it out.

And I think that there's -- I'm advocating in our world for a different stream. It's not a zero sum game. It doesn't eliminate or compete with but gets a quicker access to a more lower level sharing environment going on that before you get to the intel side. And Dr. Morris can keep all the information he needs behind that shield and my stakeholders can benefit from the timely and actionable information as opposed to intelligence.

So we would act in my perspective as a gateway of switching that back and forth, not collecting it or making it more information. When I say information I'm talking about the dots, if you will. I also would like to see it made more palatable and more useful to the operators that we deal with in the Homeland Security operators world.

For example, I recently -- I don't know how many reports and books and columns and data that I've read about the travels of the 9/11 highjackers and Mohammad Atta and his gang and it wasn't until I saw a very simple map the other day that had the lines of the points between which they had traveled that it very quickly struck me in an entirely different way, in a much more deeper understanding because it was in a graphic form. So I think that, again, rather than make it -- making it more sophisticated in a classified form we've probably got a lot of fields to plow and make productive just by transferring the data that we have already that's unclassified and open source into more useful forms.

We can use that information as a strategic planning tool to establish what normal activity baselines are so that when threats do seem to be possibly become predictive threats to track trends. We can manage incidents. The reference to study on how that's better used will be welcome in my book because the situational awareness during particularly an incident like Katrina is critical to the operation of our all hazards system, and we can start to build a holistic view of the systems that we are responsible for, the critical infrastructure that Al mentioned, for example, not in a stove piped individual form but in a holistic way that the Secretary, the President, the others involved can get it at a glance just better data as to what the status is.

So, again, the avenues I'm advocating for in our shop are not new sources. I don't believe they raise a lot of privacy issues, in fact. We're looking at how we can use that data, the operational information we may already have, in ways that are just more useful and more user friendly to our state and local partners because they're the ones who are

making the on the ground decisions. The federal government doesn't own a lot of these systems that we need to produce.

In Al's world, of course, everyone's probably heard that 80 percent or so of the critical infrastructure is privately owned. In our world the state and local authorities are operating the critical infrastructure from a government continuity standpoint and I think probably rather than new privacy concerns or new techniques of collection or the other more sensitive areas, what we really need is a new culture that gets all our partners thinking about how to share what we already have in a better more useful way. So with that, again, adhering to our more questions and less talk, I'll stop and be happy to take questions.

Ms. Sotto: Thank you very much. We appreciate your participation. Mr. Harper.

Mr. Harper: I found your perspective on these problems very appealing, frankly, because I'm not an expert in security information sharing or secrecy but I was asked once at the turn of the year what's the most important acquisition you might see in the national security area during the next year and the questioner probably expected me to rattle off five different acronyms of different programs. And I only had one, I said, instant messaging, IM. Create a secure IM for national security people at every level, let them do whatever they want with it. Let them talk about, you know, how long till the retirement date as much as they want to, but one day someone's going to say to someone else, the weirdest thing happened, someone else is going to see or hear it and say yeah I saw a weird thing too. It's an organic process like that that I truly believe is going to generate the information and to use a tired phrase connect the dots rather than a deductive.....

Mr. Lunner: Yeah.

Mr. Harper: .....intellectual, top-down, expensive program. So I really think I like what you're saying about the say this stuff would work.

Mr. Lunner: Thank you. On that point, with all due respect to Dr. Morris and his cohorts in the intelligence community, again, I have this debate with him all the time, to me the product that comes out of this sort of exchange is not an important in an intelligence sense as the fact that we're establishing that conversation and that free flow of sharing. If we're about establishing an information sharing environment we have to have more relaxed, trusting relationships in these ongoing conversations, and if this is the way to do that I think we ought to pursue it.

Mr. Martinez-Fonts: If it's okay I'd like to just add something on that because I think a word that Chet used and I neglected or left it out but it's really the trust that is developed in the process of getting that information out. It's very important. A very good example of -- and this is not as secure and all that -- but Homeland Security information network, CI, critical infrastructure, is a very good method that has proven

itself in regions of the country. It's not out everywhere but what I like to say is that talking about the sector coordinating council so they can reach, you know, a mile -- an inch wide and a mile deep. If something happens to the nuclear power companies, they'll all get it right away. If something happens to the banking industry, something happens to the postal service, they'll be able to reach out. We have some other side which is fact Chet's side that can reach on a regional basis. If it happens in Dallas they get a pretty good way, the police, of reaching Dallas. HSIN-CI really combines both of those by creating an exchange so that not only can we know that it's a nuclear power plant but if it's in Dallas we'd need to let the rest of the nuclear industry know but we need to let the schools and the shopping centers and people in that region and you know even further that that needs to be done. And so there are a series of those less formal types of exchanges of information and it is done almost on an IM type basis.

Mr. Lunner: I'm glad Secretary Martinez-Fonts brought that up because I neglected to mention this radical new system that I always advocate using when I meet with our stakeholders at similar discussions like this. It's called the telephone. And I tell them here is my telephone number, please pick it up and call me and let's talk about stuff.

Mr. Harper: I've heard about this technology. I'll be exploring it carefully.

Mr. Lunner: And I should also not leave you with the impression that there's some sort of great fight going on between us and the intelligence side of DHS. Charlie Allen and Dr. Morris and others there have been very receptive to this, it's just that it's a new way of doing business and we have to find new ways of making it work.

Dr. Morris: Yeah, let me comment about that actually. We are the ones who are researching the system he wants to use and will set it up for him so, we are working with him on that. The issue that you mentioned about instant messaging, in the intelligence community the message that you took into a broader context is one that some of us have been pushing very hard in the intelligence community. We believe even at the top secret level that we should have instant messaging among the entire intelligence community which doesn't exist at the moment. It does exist within different parts of it that I'm familiar with. The ability to do instant messaging around is something that I happen to agree with very much on. We're still pushing in certain areas to get that. Sometimes, how shall I put it? The government doesn't trust its people to use to use it wisely I think is probably the best way to put it.

Mr. Harper: And I think part of what's going to create an organic system is trusting them to use it for any purpose they want. Literally I think gossip is going to be the best -- some of the best sources of information connection.

MS. Sotto: Mr. Turner.

Mr. Turner: Thank you for your presentation and your time. Last week I was at an event that was sponsored by the Brookings Institution and the focus of the event was harnessing the power the oft-used phrase of information to facilitate community development. And there was an individual from a group, a community development group, from Rhode Island and they had developed a particular application as a client for the city of Providence to analyze mass amounts of data and present results and when they give the presentation the city, you know, official of the city government replied or responded, you know, this is fantastic, where did you get this data? And the response was, from you. And this struck me and a comment you made struck me, you suggested that you wanted to advocate a different information stream, a lower level of information prior to getting to intelligence, and you also suggested not only we have to confront the challenges of sharing the information but also the challenges in terms of how the information is presented, you know, to particular end users so I'm wondering if you could maybe elaborate upon that last point and discuss what you're doing to help present the information that is collected and used and analyzed in a way that's more meaningful to different end users.

Mr. Lunner: Let me cite you as an example something that we did at TSA while I was there that's sort of a prototype for this idea. And it was -- when I was first there I noticed that we got reports from the aviation community about suspicious incidents and we got -- that went to, you know, this file and we got reports from the highway watch trucking safety and anti-terrorism operation that went into this file. And then there was Coast Guard reports and maritime incidents that were considered by someone else.

And what we did was, again, going back to the holistic approach, was to take them for the first time and put them on overlaid each other so you could see at the end of the week, we encouraged our stakeholders to call us with their individual dots, and then what we would do is assemble them into a matrix so that anybody could see at a glance literally on a map of the United States that there was, you know, gee, a cluster of activity over here this week in these different domains that may have matched something that was going on in this side of the country, et cetera. That presentation, again with existing data that was already in the stream someplace, the stakeholders found very useful and were able to just see a different perspective in a more usable way. That's the type of thing I'm talking about. I think there's lot of -- there's probably -- well, I won't say a lot. I know there are, there must areas that we have yet to explore of that type of information that we have that we can bring to bear both internally and externally.

Ms. Sotto: Thank you. Mr. Wright.

Mr. Wright: In your experience to date, obviously in dealing with both state and local and also dealing with the private sector, obviously the atmosphere or relationship that we want to promote is one of sharing of information going both ways.

Mr. Lunner: Yes.

Mr. Wright: Just curious that in your work thus far if you've seen issues where state and local or private sector sources have been reluctant to share information with you because of their own either state or private sector criteria for treating things in a confidential manner or in looking to protect the privacy of their sources or whether you've seen reluctance from them giving you information because of concerns as to how either DHS or other federal agencies may in fact use that data that might compromise some of their privacy concerns. I think the committee would really be interested in that sort of information.

Mr. Lunner: If anything, I would submit that the state and local operators or stakeholders are ahead of DHS in being able to share. There's many regional efforts that have started up, fusion centers that go beyond their initial jurisdictions. I would not say that there's a reluctance in my experience.

I get, matter of fact, a series of weekly products from the various states, you know, New Jersey, Illinois, California, about here's what we're discovering in our jurisdiction this week or this day or whatever, and that's the type of information that I'm talking about we might add value to by picking out the things that would be of interest beyond their jurisdiction to share with others. So in this -- I'll let Secretary Martinez-Fonts talk about the private sector, and I know they have some proprietary concerns, but in the state and local area we have not seen reluctance. They're anxious for us to get these systems up.

Mr. Martinez-Fonts: Well, I think as I mentioned earlier, I think we have seen it on the private sector for sure and for, again, any variety of reasons from, you know, competitive to legal reasons to just their concern of our ability to protect some of that information.

Dr. Morris: I don't know if it's particularly a privacy issue. One of the issues that we have run into is that within a state it's not necessarily clear that law enforcement wants to share its information with all the other parts of the state. We, on the other hand, in DHS have to deal with both the law enforcement side of the state and the political side of the state and so sometimes we get caught within internal communications issues on information sharing among the various people. And so that issue has come up in the past.

Ms. Sotto: I'd like to follow-up Sam's question to ask you, Mr. Lunner, to comment if you will on the Matrix database which would be this giant database that states contribute to. It has -- it's received an awful lot of fire and I'm wondering whether you think this would be a useful tool for you. Have you had any input, have you had any discussions with the states or been privy to those discussions?

Mr. Lunner: Madam Chairman, I'm really not qualified to address that issue. As I said earlier, we facilitate the sharing of this information where we can. Matrix is not a particular system that I'm all that familiar with and I'll leave it at that.

Ms. Sotto: Mr. Palmer.

Mr. Palmer: Yes, first, just a comment on Jim's comment and then a question. Regarding instant messaging and similar things, it's not just gossip. I mean, one thing about gossip is that it does build trust and connections and networking inside the organization and you really need some of that. It also allows you a very cheap and fast way to prove that the system works, especially during certain shall we say not particularly national security threatening events like the Super Bowl or the Sports Illustrated issue or whatever that might generate a lot of traffic, it's a wonderful way to just beat out the system and make sure that it's working.

And I thought you might raise a concern, one of you, that most common technology for this is a central server through which all messages pass and that scares the heck out of a lot of the private sector saying oh no it might be XYZ confidential information flowing through that other company's server. And you don't have to do it that way so that shouldn't be a stumbling block.

My question is regard to audit. While I'm certainly an advocate of giving S & L & T everything they can get that is particularly if it's actionable, how do you handle the audit? And I bring this up because of a personal experience. My high school reunion was looking for an individual and we couldn't find him. We hadn't seen him for 30 years. And so someone said well I know Bill in the state police and they actually got Bill to look the guy up and we found him. And he really didn't want to be found because the fact that Bill could find him well meant he was on certain databases. So the question is, how do you in this effort to drive the information down, how do you make sure or can you or are you not even bothering to try to make sure it is used appropriately?

Mr. Lunner: Well, we're a gateway in my office. I don't have access to any of those sorts of databases unless you want to count Google. I would take the information in my -- that someone else has generated from one of the states or one of the departments or one of the Homeland Security advisors or some of the information that's been cleared by the people in Dr. Morris' shop for distribution outward and act as a switch and try to get that out in as timely and useful fashion as possible. Our office doesn't have access to the sorts of information you're talking about.

Dr. Morris: Just a comment about that. You know, it's an interesting question that you ask about looking at data and one of them I present is this one. As a matter of record, all real estate transactions any place are public record and I as a private citizen can go into Arlington County and look up any transactions that went on. I as an intelligence officer

though gets into a very shady situation. Can I go in there and look up a particular person that I am interested in and go in there and do that? Now we're getting into a shady area. And so and I don't know the answer to that. It's a question I presented in a discussion we were having the other day on this topic. As a private citizen I can walk in there. As an intelligence officer I'm not so sure.

MS. Sotto: Thank you. Mr. Beales.

Mr. Beales: Thank you. I wanted to focus a little bit on the private sector information and the private sector information as an input. For Dr. Morris and for Mr. Martinez-Fonts, what kinds of information would you like to get from the private sector and from what kinds of institutions, I mean, what kinds of companies?

Mr. Martinez-Fonts: Let me address it from let's say the critical infrastructure which are probably the redundant, the most critical ones that we would want to get. If there were information on where their vulnerabilities are in particular, what might be something that could be exploited, and let's talk again very much on a terrorist side of things, we would want to know that. Where there are, you know, numerous chemicals that are stored where there could be single point of failure, if you could have an attack on one point that would put out the, you know, all the telephones in a major city, if you could look at water purification, food, all of those things, that would be the kind of information that would be very helpful to us to help them make sure that we can then strengthen that vulnerability and make sure that the consequences that occur as a result of it are not as damaging.

Dr. Morris: The kind of things that we generally look for, one, is exactly that, is an understanding of the threat that they perceive or the kinds of threats that they might -- or vulnerabilities, I guess that's a better word for it, such as allows us as we go through the traffic and we're investigating groups or people that we can spot the kind of things that would come up that we would say hey they may know something, they may see vulnerabilities, they're talking about this. It helps us have a better understanding of the knowledge of the adversaries or the bad guys as to what their knowledge of a particular industry has to be.

I think the other area is suspicious activities. We continue to be interested in suspicious activity reporting and correlating what's happening at a power plant and people may be doing surveillance on a power plant in Washington State and another one in Florida, and how do we bring all that together effectively. There are a couple of areas.

Ms. Sotto: Mr. Alhadeff.

Mr. Alhadeff: Thank you. I guess this question was generated mostly by the example you used of the, you know, the guy with the yellow jacket or whatever, the

description was, and it made me think that in many of the descriptions we've kind of talked about people that have the security clearance, we've kind of heard about this is classified and it's non-classified information, sensitive but unclassified information, and a lot of those classifications have the normal information security components that one would expect and what I'm not hearing a lot about is how can we use the identified information to actually find some of the, you know, to do some of the targeting because if you're going to scan against a data set, scanning against a D-identified data set to the extent that there are behavioral patterns that you are looking for may be the best way that you minimize the access to information. Because it's not just the inside and the outside but it's also the need to know which all of you have in one way brought up, but I kind of get the feeling that that need to know is intention and when we start having the concept well I'm cleared then the need to know somehow becomes a little bit diminished. And I guess I'm trying to figure out how we can maximize the use of D-identified information and how we can also maximize the need to know limitations to still be effective in what you're trying to do but as perhaps limited in scope in what you're actually capturing of detailed information.

Dr. Morris: I'm not sure I know how to answer your question. I think you have to look a little bit at kind of what are we doing quite often in the intelligence business today, and I don't mean just DHS, I mean all the intelligence business relative to terrorism. What we're spending an awful lot of time doing is looking at particular individuals. Then from that individual, looking at networks of individuals. And from that looking at groups and what they intend to do. And from that trying to basically ferret out from that hints of things that are not obvious to us by making connections, making connections to places, and we're spending a lot of effort in the community and I think in some cases very successful efforts in the community in making those kinds of connections. It is difficult to work in the without names associated with that. It really doesn't help you a lot.

Now, can you keep it in a database in that way until you can make a connection to the substance of this person was in this spot at the same time this person was in the spot, does that make a connection between them? Potentially. And those kind of things are done also. But for the kind of -- the thing that makes the counter-terrorism business different from the kind of intelligence in things we have done in the past it is very personal. We are chasing people, individuals quite often, and that gets us right up against privacy laws real quick and rules. And so I don't know how to chase people without names and that's I think part of the problem we're faces with.

Mr. Alhadeff: So from what I'm understanding, it's where there had been previously a lot of top-down concepts of using profiles to try to match people with profiles as opposed to names, that current methodology is actually bottom-up in terms of finding identified individuals and then building nexus comparisons of relationships so

that the profile aspect is less in use now than the kind of who you know, what you did, kind of concept?

Dr. Morris: What I see, that's a major part of it, yeah. We spend a lot of time trying to make connections, you know, bad guys associate with bad guys and we need to make those connections. I mean, history has shown that's pretty much the case. Trying to find a bad guy out of nothing without connections is very difficult, if not impossible.

Ms. Sotto: Thank you. Mr. Barquin.

Mr. Barquin: I wanted to ask a question about a slightly different area and that's the area of certification because it goes right back into this issue of identifiers of individual information and obviously it's going to be hitting very directly first responders at the state and local level as well as the private sector and especially as we're facing some of the natural disasters where all of a sudden you need someone that is certified as a healthcare provider to allow them to do this, that, or the other. And the specific question here is, how are you thinking about this in the context of this information sharing environment and what type of guidelines are we going to provide to be able to embed some of these privacy values as we build these certification systems?

Mr. Lunner: I know there's a nascent effort in the department post-Katrina on those issues because of the access problems that some utility workers even law enforcement and first responder neutral aide guy who responded under EMAC had difficulty getting to the scene because there's another issue with physicians and nurses and people in the health field who are trying to supplement the locals and whether or not their licensure is up to speed in that jurisdiction. I've never heard it in the connection of what you were talking about. Usually the difference I think between the privacy issues that we face in other areas and here is that those people are volunteering, they want their information in some central location so it can be checked, and it's not something that we're pulling from them. It's useful to them and they want us to hold it in some repository so that we can verify that yes indeed that person is certified in the state of whatever and you should let them in at the scene of the incident.

Mr. Martinez-Fonts: The situation that we've run across much more has been with credentialing per se, just being able to get into the area. This was an issue at 9/11 and New York has developed a very robust program. Tom Dinanno, who's Deputy Assistant Secretary for Infrastructure Protection, is putting together or has put together a group that is looking at that, especially after Katrina.

Some of the issues that we ran into with the private sector with the parishes in Louisiana in particular which I gather are more autonomous than counties in general, people literally needed, you know, five and six and seven approvals or credentials to get from one county to the other to reach New Orleans coming from Texas or coming from

Mississippi and so on. So there's been a big issue on that and there's a lot of work that's being done.

Again, we had not focused so much, as Chet said, on the certification side of it although we know that that's an issue. I'm going to say if we could probably solve, kill two birds with one stone, if you had the right credentialing. But it is a very complicated issue when you have in a different shifts of people coming in and how many are allowed. First Chicago, Chicago First, which does a group with the financial sector in Chicago has also done a very good job on credentialing.

Mr. Barquin: If I could just follow-up because the, at some point, it was pointed out to me that some very significant percent of truck drivers that needed to be certified or credentialed also had in many cases a record and the question was how legitimate and how ethical would it be then to start having scope creep if you will of that information gathering and it's a question of thinking about what kind of privacy guidelines you're going to put in place before the systems go up.

Mr. Martinez-Fonts: Yeah, truck drivers, by the way, and Chet could probably talk about this a lot more than I can, but have been a real, real issue. I mean, there is just a dearth of truck drivers and they need to get certain certifications, in particular, hazmat certifications, and may people won't hire you without the hazmat. And depending on your record with your state and local group, you may get knocked out of that box and, therefore, so that it does present a number of problems.

And the issue always is as you say from a privacy point of view do you want to just be able to send in a name and you get a red or a green light and then you check, you know, why did I get the red as opposed to getting the green and all that but a transport worker, identification card is.

Mr. Lunner: Well, it's TWIC program is where this discussion initially began at TSA in the wake of 9/11 and it involves truck drivers, it involves dock workers in ports, anybody who has multiple jurisdictions to go through and it's not as simple, like many things, as it looks like at the outset and what the discussion eventually gets to is not only -- a couple of important areas, we probably don't need to have credentials on every truck driver in the United States, but we have to decide at some point those trucks carry some very, very sensitive material around the country, and the people who are handling those trucks and have access to those trucks probably we should have some better understanding than just the passing a driver's license.

And, secondly, then to what to give them access? There's a whole different area that's not settled policy I don't think about okay you've got this care, where does it get you? Oddly, I haven't heard as much, and again, you're in a different paradigm than we usually have these discussions, the privacy concerns are not what I hear voiced so much

as what disqualifies me? You know, does that barroom fight that I had in 1962 going to keep me from earning my living? And so that's where the focus of the conversations have been that I'm aware of.

Ms. Sotto: Ms. McNabb.

MS. McNabb: One of the things that one of you mentioned that you want to get from state and local and private sector is report the suspicious activities related to critical infrastructure. For example, who defines what are suspicious activities? Do you give them guidelines? Do they tell you? Does it change as the threats change?

Mr. Lunner: I'll give you an example, and there are, depending on the sector, will be various, you know, variations of this but in the highway watch program, for example, that has been very useful, the truck driver -- it's more than truck drivers, it's truck drivers, school bus drivers, toll booth collectors, anyone in that venue, in that domain of the transportation network volunteers to take this highway watch training and in the training they're given an 800 number and a PIN number so that we know it's not some random, you know, fire alarm puller calling in, and, secondly, they're given training about how to keep themselves safer in that environment that they're operating in and then on top of that what we think suspicious incidents might entail.

It's not -- it's an inexact science, you know, it's more of an art than a science but it's pretty much tailored to the areas that you're working in and it will involve, you know, why is that person taking photographs of your truck or why is that person following you or, you know, generally I don't think it rises to any specific hard definition of suspicious incident. It's pretty much what you'd think of if you and I sat down and said what are suspicious incidents that truckers should look for, it's generally a consensus sort of a list.

Mr. Martinez-Fonts: In the case of critical infrastructure it does get a little bit more defined and particularly -- I'm trying to think of large facilities that have lots of exterior fencing and the like, any kind of casing, photographing, people trying to get in just sort of acting stupid and walking up and saying I need to go see Mr. Smith, you know, who are you, what -- a lot of that kind of stuff there is -- and by the way, as specific information is found, we hear there is a threat against the electricity sector, then we warn.

Mr. Lunner: Additionally, an important point that I just thought of is that that training also includes and all of the guidance that I've seen going on includes a caveat that a person's appearance or apparent ethnicity or dress or that sort of thing does not constitute a suspicious incident and we're looking for behavior not appearances.

Ms. Sotto: Thank you. Mr. Harper.

Mr. Harper: A lot of the discussion about the information sharing environment is heavy with jargon and difficult to understand, and I think I've found the reason for that. It's because the statute is heavy with jargon and difficult to understand. I was amused,

frankly, when in the debate over the bill they changed it from information sharing network to information sharing environment and I thought that might be to bring some more people onboard who thought this thing would be good for the environment so they should vote for it. But I am concerned with the product that Congress gave us and there should be no mistaking that it's Congress' product. And so it's not meant as a criticism or concerned expressed about any of you or your programs. The definition of terrorism information is essentially limitless and if someone tried to enforce it someway or other I don't think they'd have standing to do so. Several places the statute appeals to the legal standards relating to privacy and civil liberties but one of you mentioned that the environment, whatever it ends up being, wouldn't be subject to FOIA. I wonder if it would be subject to the Privacy Act in any sense. What are the privacy laws that, Dr. Morris, you mentioned up against. Are you subject to those privacy laws under this statute?

Dr. Morris: Well, I think that we are. I think it depends on to some extent that the one that we continue to get into is -- the intelligence community really isn't. Okay? But the non-intelligence community is. And our job unfortunately is caught in between those two and how do we do that effectively. And we deal with that within intelligence and analysis and how we handle every day. I think that the issues of privacy with respect to the information sharing environment are real, I think they are things that we're trying to handle within there. There is a specific guideline I believe that deals with, that came out of the White House that deals with making sure that how we deal with privacy within this domain. I think we take it seriously but there are different rules and regulations and even cultures that you deal with once you cross that line between intelligence and other things, law enforcement, for example, and we're still working through those. But I think we're conscious of the fact that they need to be worked.

Mr. Harper: You have a report due in another three months, preliminary report, under the statute, is it going to include extensive discussion of the privacy issues and privacy laws?

Dr. Morris: I don't know. Just because I don't know one way or the other. The privacy issue has not been a major part of our information sharing council discussions to date only because we have so many things we're trying to do within that that it's -- I come out of the meetings every week and shake my head about how am I going to get all that done. So there's an awful lot of activities that are called for within this. Privacy is not one that we've dealt with as a group yet. I know there've been other discussions going on within that. I know the privacy office has been involved very heavily in some of those. It's just that we exactly what's going to come out, I can't tell you. I don't know.

Mr. Martinez-Fonts: I'm the one that brought up the FOIA issue but I don't handle the PCII but the answer is I don't know. And I'd be glad to get back to this group how the privacy laws impact the PCII information.

Dr. Morris: One of the specific things that we've gotten into is that intelligence systems are exempt from the privacy laws, however, DHS has not exempted its intelligence systems so we do privacy impact systems against our intelligence systems in DHS.

Mr. Lunner: In an important distinction, the PCII is about things not people. It's about infrastructure.

Ms. Sotto: Mr. Purcell.

Mr. Purcell: Thank you. Just as a follow-on, Dr. Morris, you just mentioned that you are conducting or have conducted privacy impact assessments against your, the resources, the databases, or at least in part or some of those and I'll ask for some clarification on that but I want to ask more generally and kind of comment also that the committee believes strongly that the privacy impact assessments are very usable process and a very valuable process to understand how to kind of thread some of these needles and to untie some of these knots that you do run up against and gives exposure not only to the privacy office for leadership but also gives the committee some information about how perhaps best to lend some of our resources to help the privacy office in this area. So if you don't mind, I'd like to understand comments about where you are in the PIA process within your different areas.

Dr. Morris: Well, let me start. I think we're just getting into it. I think we -- my own personal experience with, we had some discussions with the privacy office in trying to -- there's a requirement that we do a PIA for any systems that we built and we're trying to meet that.

What we've found to be the difficulty in that is that the some of the language between the intelligence community and the privacy sector don't always match and how you deal with that. And things like how are people going to be able to remove data from your intelligence system? Well, I'm not sure that's a question we can deal with here. Now, we certainly want to deal with the right questions but those are some of the kinds of things that come up as we're trying to bridge that gap between the two. So we're actively involved in discussions of it. We'll see how it comes out. But establishing the kind of dialogue that allows us both to -- for the privacy to understand king of the intelligence community and the intelligence community understand the priorities of the privacy I think are key factors that we need to deal with in that.

Mr. Martinez-Fonts: Just given the nature of the information that we're handling, we have not had any specific privacy issues that have either been raised or brought up or are dealing with.

Mr. Purcell: Sorry, does that mean that you're not filing an impact assessment because you're not -- you don't have systems of records?

Mr. Martinez-Fonts: Correct.

Mr. Purcell: All right.

Ms. Sotto: Jim, along those lines, are you -- do you continue to be interested in a written follow-up to your question now that you know that we're talking about things not people?

Mr. Harper: Yes. Actually, I mean, I'd like to see it, you know, dealt with. It doesn't need to be to us but perhaps if the 180 day report were to -- because I don't want it to demand a lot of paperwork from you but I'd like to see the issues addressed.

MS. Sotto: Good. Thank you. Any other questions from the committee, for the panel? Joe.

Mr. Alhadeff: Just actually the last statement was kind of very interesting in the sense that I think it would be tremendously useful for us to understand where there are disconnects going on with the privacy impact assessment process and where it's running up to something that is not applicable as written to the intelligence community because I think one of the concepts is it, the PIA is a learning process for everybody when you do the first one, and kind of understanding where it may need to be tailored or where it may need to be explained in a different way because I think there is the concept of multiple lexicons going on here. So I think, you know, the experience of someone dealing with the PIA and where the fit doesn't occur would be tremendously valuable for us.

Dr. Morris: And I'm trying to figure out the same thing. I mean, I think that's the issue, I mean, the classic one is okay can they get to review that data. Well, not if it's classified. Okay? And so developing that dialogue and understanding that is certainly one of the things that I, and my staff, are really trying to get a handle on right now.

Ms. Sotto: Mr. Lance Hoffman.

Mr. L. Hoffman: Yeah, at the risk of using up the last amount of time. I'd just like to second or third your comment because it really struck me what you said also about the discussion between two cultures. It may just be that you don't even need to right away do a PIA. I'm not saying you don't have to do it but I'm saying not next week because if there are semantic differences or something like that, I'd be interested in what activities you've undertaken so far. You gave a very general discussion of what you've done and I'd be

interested in if there's anything specific you've done or if there isn't what you might do either with the privacy office or other entities to breach this cultural gap.

Dr. Morris: Well, as I said, I'm just learning myself about this. I know we had a project that's really a project to develop analytical tools to support our analysts in going through data and how we search and how we catalog, et cetera. My people have been working for, what, more than nine months with the privacy office trying to write an acceptable PIA for that project and we get into these questions like, for example, how are people going to be able to review the data in your database to see if it's correct. Well, my database is classified. Okay. I don't know how to quite deal with that. The issue comes to how can they remove data? Can they demand it -- and these are the kinds of things we just have to work through and we're trying to do that. And we get some questions back from the privacy office, excuse me, that I don't even know -- this doesn't make sense in my world. I don't know. So this is the kind of dialogue that we're trying to have happen. And I agree with you, but I'm working through it myself right now so we're trying to get there.

Ms. Sotto: Thank you. Mr. Beales.

Mr. Beales: I was just curious about following up on the comment you made earlier. What is it you run up against that is -- that you think does or may restrict your access to public record information?

Dr. Morris: Classical intelligence communities, what rights does the intelligence have to view U. S. person data and search into U. S. person information? Now, the Office of Intelligence and Analysis under the Homeland Security Act has very broad powers in that. We have the right to see any information that has a nexus to homeland security. It doesn't matter whether it's U. S. person data or foreign intelligence data. But those are kind of unique responsibilities within our office. We on the other hand have to deal with the counter-terrorism center, we have to deal with the other parts of the intelligence community and how that information gets shared or what databases it moves into are very critical questions to us in dealing with that. I don't know -- somebody asked me, in fact, I've asked other people, where is privacy getting in the way of us doing our business? I haven't been able to identify that and which is probably good. On the other side, the privacy office is probably asking are you going over the line somewhere so and that's the normal contention here that I think we all have to continue to address and address up front.

Ms. Sotto: Thank you. Ms. Lemmey.

Ms. Lemmey: Well, Lance, first I have to disagree with you that I don't think that delaying the privacy assessment is necessarily a good thing. I do think that Joe brought up the issue of is a challenge and that's important. Having stepped into this debate coming

from a privacy advocacy perspective it was fascinating for me that our language didn't match up initially and where it didn't was interesting but what it does force is, one, really a heightened sense of oversight and where does oversight happen if it's classified and how does it happen within the system that you have currently, and, two, it puts a lot more burden on collection and tasking in the earlier phases because once the information is in it's incredibly difficult to get out.

Whereas from the private sector perspective most of us who are on that side of the house said well you can remove it and you can access it and that became a normal part of our lexicon. And that it also goes back to the earlier conversation about sharing with other organizations who then you have to move into another oversight body and another set of events so that if it's wrong in the first place you're compounding wrong with wrong in every organization and agency it goes to which is why all the pressure's on the privacy really happen at the front end and really do force more of this design integrity requirement specifically because of where our lexicons don't meet each other and where the processes are at cross-purposes. So perhaps it encourages a more thorough set of discussions is what it sounds like to me here about that front end part of the process and particularly on the oversight issues.

Ms. Sotto: Any comments from our panel? Okay. I'd like to thank you very much for joining us. Your remarks form a terrific building block for our afternoon discussion which will be focused on operating within an information sharing environment. Couple of administrative points. We will now break for lunch. We will resume promptly at 2:00 o'clock. Please be in your seats by 2:00 o'clock. There is a food court located on this floor and also a number of restaurants in the vicinity. For members of the committee, please report to Hemisphere B for lunch and I would also ask members of the committee to please focus on the framework paper which was issued in revised form, I think it was actually printed yesterday or today. We will be having a discussion about adoption of that paper after lunch. Thank you very much. (Lunch recess)