



Homeland Security

DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
FULL COMMITTEE MEETING
WEDNESDAY, SEPTEMBER 20, 2006
Transportation Security Administration
Town Hall
601 South 12th Street
Arlington, VA 22202

MORNING SESSION

EXECUTIVE DIRECTOR RICHARDS: Good morning. My name is Becky Richards. I'm the Executive Director of the Data Privacy and Integrity Advisory Committee, and we're going to begin this meeting, and I'll turn it over to Howard.

CHAIRMAN BEALES: Thank you, Becky, and good morning everyone. A couple of housekeeping matters before we get started. First, please turn off your cell phones. I'm sure you have a really cool ring tone, but I'd rather not hear it. Second, bathrooms are out the door and down the hall on the right. And, third, as is our custom with our public comment at the end of the meeting, if you want to speak to the Committee at the end of the meeting, you need to sign up with Lane Raffray back there somewhere. You know, at any time over the course of the day, please sign up with Lane if you'd like to address the Committee at the end of our session. I want to welcome our new members to the Committee. We are delighted to have you. Those of us who have been hard at work on a wide variety of projects are glad to see new hands. And we promise to keep you busy and look forward to your contribution. This morning, we're going to start with hearing from the new Chief Privacy Officer, Hugo Teufel, who we welcomed to the first meeting of the Advisory Committee. And, again, congratulations on your appointment. Hugo was appointed by Secretary Chertoff on July 23rd of this year. He also serves as the Department's Chief of Freedom of Information Act Officer. Prior to joining the Privacy Office, Mr. Teufel served as the First Associate General Counsel for General Law at DHS. And prior to that, he was the Associate Solicitor for General Law at the Department of the

Interior. So, Hugo, welcome. We look forward to hearing the report from the Privacy Office, and we look forward to working with you.

SPONSOR TEUFEL: Ah, yes. Technology, it's a wonderful thing and part of the Office's mandate under Section 222. It's great to be here. This is not the first time that I have met with you all, but the previous times would have been in my former capacity as the Associate General Counsel for General Law. So good morning, and greetings to the Chair, Howard Beales, and Vice Chair Lisa Sotto, and to the Committee members. I especially want to welcome the Committee's new members: Ana Anton; Thomas Boyd; Mary De Rosa; Renard Francois; Neville Pattinson; and Larry Ponemon. Hopefully, I pronounced everyone's name correctly and, if not, I sympathize with you. Well, it's easy to pronounce Teufel, and spell it, too.

This is my first Committee meeting as Privacy Officer and, although we are still getting to know each other, I wanted to extend my support for the important work of this committee. You each represent the very best in your fields, and we very much appreciate the time you take away from your jobs to participate in the work of this committee. I look forward to working with this expert body to further the mission of the Privacy Office and of the Department. Defining privacy and the mission of the privacy officer. Like my predecessor, Nuala O'Connor Kelly, I believe that the Privacy Office must build a culture of privacy across the Department. We frame the mission of the office as securing the homeland while protecting privacy. That's very important because, while we are at war, and some say a long war, and in any war certain compromises are made. There are some things we ought not compromise. Establishing the culture of privacy at the Department will ensure that the Office and the Department are successful in their mission. I believe very strongly in the mission of the Privacy Office, which is why I'm here today.

Why is it important to protect privacy? I believe that respect for individual privacy is a core value of free society and one of the fundamental issues that DHS is fighting to protect. Privacy demonstrates our respect for human dignity and other values, such as freedom of association and freedom of speech, property rights, and the concept of liberty. It is these values that distinguish us from those who seek to destroy us. Of the things we value as Americans in our constitutional republic, privacy is perhaps the most difficult to define. In our country, the concept has been fused with the concept of information privacy, which interprets privacy in terms of the appropriate use of personal information. But privacy is also a way of drawing a line in how far society and government can intrude into a person's affairs. The loss of privacy can be incremental and gradual. Each intrusion may seem unimportant or a necessary tradeoff for some other seemingly competing principle. But, ultimately, once lost, it cannot easily be recovered. Its loss can change the very nature of how we interact with each other and with our government. Another way to view privacy is through the concept of trust. If failure to facilitate privacy breeds an

inherent distrust of an organization, DHS must have the trust of its partners in the private and public sectors; state, local, and tribal governments; and citizens and other individuals who travel to, do business with, and generally interact with our nation. Understanding privacy in this way, coupled with our organic statute, Section 222 of the Homeland Security Act, it is obvious that the Privacy Office has a broad range of responsibilities. Fundamentally, any DHS program that touches on the collection and use of personal information will demand our attention. And most programs at the Department impact privacy. I've now served as the Chief Privacy Officer for about seven or eight weeks, a fairly eventful seven or eight weeks I might add, especially the first two or three. And I've made progress as I look at what I want to accomplish while serving in this office. I can tell you that I will build on the foundation laid by my predecessor to ensure that at the operational and strategic levels of the Department privacy is a part of the solution to the complex challenges the Department faces. In the short time that I've been in this office, I've worked closely with the Privacy Office staff, a very capable and dedicated group of individuals and professionals and the best, I would say, from throughout government, who came to work here at DHS. To assess the operations of the office and to prioritize our efforts, we have parsed our organic statute and compared our legal mandate with the Office's current functions and duties. We are also looking at workflow to ensure that we are timely in our efforts. As well, I have begun meeting with each of the heads of the DHS components to offer our assistance and to make sure that privacy is an important consideration within the senior leadership of the organization. Key officials include, of course, the Secretary and Deputy Secretary, General Counsel, Assistant Secretary for Policy, Undersecretary for Management, CIO, and CSO, but also the Inspector General and the CIS ombudsman. And I meet regularly with the Civil Rights and Civil Liberties Officer. In addition, I have met with the senior privacy and civil liberties officials of the Department of Justice and the Office of the Director of National Intelligence. And soon I will be meeting with the senior official from Department of Commerce initiate the relationships that we'll need to address privacy in the context of important cross agency initiatives, such as the development of an information-sharing environment.

There are no smoke stacks in the privacy and civil liberties community within the Executive Branch. So how do we go about making privacy an operational consideration? By working closely with DHS components to consider privacy throughout the life cycle of each information system within each program; by urging programs to begin to consider privacy at the design stage. Moreover, as programs make changes that touch on personal information, programs need to consider how those changes impact on privacy. Don't think of privacy of an issue you address once and then can put on the shelf. As you know, a key tool is the privacy impact assessment. As you know, as well, this office has developed a template for PIAs. What you may not know is that that template has been adopted and adapted by other federal agencies. OMB, for example, used our PIA as a

model in building the PIA for HS PD, the President's homeland security policy directive, to develop a common identification standard for federal employees and contractors. Another important tool we use is the OMB 300 Budget Investment Process, which serves both as a carrot and as a stick within the Department. As part of the OMB review process, OMB 300 review process, each investment is required to submit a privacy documentation in order to receive funding, specifically OMB requires a privacy impact assessment and a system of records notice for each system, unless an exemption applies. The Privacy Office reviews every OMB 300 investment to determine whether all required privacy documentation has been completed, approved, and published. I know that my staff works on the OMB 300 review and is very pleased that they have just completed their annual review, which has consumed much of this last summer. In addition to the operational bread and butter work of the office, there are a number of high-profile matters that we are and will be considering. Just to name a few, Western Hemisphere Travel Initiative, Real ID, PNR, among others. Doubtless, we will be involved with the Secure Border Initiative, which, if you believe the Washington Post, a contract was recently awarded. There will be a lot of public and media scrutiny in what we do, and the Privacy Office will be involved heavily in these matters. In closing, I'm honored to head the Privacy Office, as I recognize that it has a critical role to play in the mission of this department. I will look forward to reporting to you at the December committee meeting in more detail on the work of the office to build a culture of privacy at the Department of Homeland Security.

So, unless there have been changes to today's program, I'd like to review with you what we'll be doing. This morning, we'll be hearing from Mark Robbins, Executive Director of the President's Civil Liberties and Oversight Board. Tamara Miller from the Transportation Security Administration will be here. Kathy Kraninger, Director of the Office of Screening Coordination, will be here. And I believe we've had a change, and the Deputy Secretary will be joining us, instead of the Secretary. So this afternoon, we have two panels: one on the important topic of redress, where we will here from James Kennedy of the TSA Redress Office; and Debra Rogers of the U.S. Citizenship and Immigration Services Customer Service Office. I hope I don't have to say that three times very fast; I might have difficulty. The second panel will focus on data integrity, and the panel includes Jennifer Barrett, the Chief Privacy Officer of Acxiom; Bob Ryan, Director of Government Relations at TransUnion; and Xuhui Shao of ID Analytics. And, now, it's my honor to introduce Mark Robbins, unless you would like to do so, Mr. Chairman. I guess I will. Okay. On March 14th, and he's coming to join us, on March 14th, 2006, the Privacy and Civil Liberties Oversight Board appointed Mark A. Robbins of California as its first executive director. Mark is a member of the White House staff and oversees the board's professional and administrative support staff. Prior to taking this position, he served as a general counsel at the U.S. Office of Personnel Management from 2001 to 2006 and was on

the Bush-Cheney transition team in 2000. And I've got to tell you in both of my prior jobs, first as Associate Solicitor for General Law at Interior and then as Associate General Counsel here at DHS, I've had the pleasure of working with Mark. He is a true professional, and we are very lucky to have him in public service. From 1988 to 2000, Mr. Robbins practiced law in Los Angeles, California, specializing in civil litigation. He was a candidate for the U.S. House of Representatives in 1992. Mark previously served as Deputy Associate Director for Presidential Personnel at the White House during the Reagan Administration, '84 to '88, and as a legislative assistant to Congress, David Dreier, '82 to '84; and John H. Roussetot, '79 to '82, both of California. Mark received both his BA in international affairs and JD from George Washington University in Washington, D.C. And with that, Mark?

MR. ROBBINS: Thank you, Hugo. I appreciate this opportunity to be with you all here this morning. I thought what I would do is give you a brief kind of round-up of what the Board has been doing in its first six months since the members were confirmed, give you an idea of where we think we're going at this point. And then if you have any questions, I'd be happy to address them to the extent I can. I know that I have been reaching out to a number of organizations and individuals. For instance, Mary, I think you can probably give this speech for me. So if I'm duplicating anything that you all know already, I apologize. I figured I'd just let it all out now. The Privacy and Civil Liberties Oversight Board was recommended originally by the 9/11 Commission Report, and it was included and authorized in the Intelligence Reform and Terrorism Prevention Act of 2004, which President Bush signed into law in December of 2004. There has been some criticism over the lag time between December 2004 and the Board's first meeting in March of 2006. I will tell you the Intelligence Reform Act, as you all know, contains some pretty important pieces of legislation and priorities. The Administration did prioritize what it needed to do. Obviously, the stand up of DNI was very important. And while I'd like to think that my Board is the most important group of people in the world, certainly there were priorities that had to be dealt with first. The President nominated the chair and vice chair. Those require Senate confirmation in June of 2005, and the Senate confirmed them in February, and we had our first meeting about three weeks later. The members are a diverse, very energetic, intelligent group of people. The chair is Carol Dinkins. She's a partner with the Houston office of Vinson Elkins. Until Janet Reno, Carol was the highest-ranking woman at the Justice Department. She served as Deputy Attorney General under William French Smith in the Reagan Administration. Our vice chair is Alan Raul. Alan is a partner with the D.C. office of Sidley Austin. He actually has published and lectured on privacy issues. He started his career as associate counsel to President Reagan at the White House, and then was general counsel at both OMB and the Department of Agriculture. Our members, which are not confirmed -- they're presidentially-appointed but not confirmed by the Senate -- include Laney Davis, former special counsel to President

Clinton; Ted Olson, former Solicitor General; and Frank Taylor, a career Air Force Officer who retired as Brigadier General and then served as Assistant Secretary of State for Colin Powell on security matters.

It's a very, very good energetic group. And one of the things I found, and it's always an executive director's worst nightmare that you're going to get five very energetic or a dozen energetic people going in all kinds of directions, and I can tell you that these five individuals all share the same commitment to this particular project and a passion for doing it right. None of them signed on to be a fig leaf, none of them signed on to be a rubber stamp. They're part-time, but the job itself is not part-time. It takes a lot of time and a lot of effort and a lot of energy, and I'm pleased that they're dedicating what I think is necessary in order to get this job up and running. They also, interestingly, get along. It's wonderful to be in meetings with all of them. It's fun. I look forward to it. There's a lot of hard work putting meetings like this and like what I put together on. And when they actually start and you get these five individuals together, the chemistry works. Their strengths compliment each other. Their interests compliment each other. And I think anybody who has been in a meeting with that pick up on it almost instantaneously. Four of them are lawyers, rather successful lawyers, so I always apologize to people in advance when they're coming to address the Board to be prepared for the litigator's method of questioning. They don't wait until the end for questions and answers. There's a lot of back and forth. And I've had people come up afterwards saying, "You know, I don't think I got the points made. I don't think I got everything that they need to understand this." I said, "Well, did you cover everything in your notes?" "Yes." I said, "They'll get it. They'll be able to take it in the order that they wanted it and put it all together." And it keeps me on my toes, and it always frightens the people addressing the Board a little bit in advance. But it's a great group. Our mission is both very broad and very specific.

We have three specific charges. The first is to be part of the development, implementation, and review of the guidelines for the information-sharing environment, which is a project currently underway. The second is to make an annual report to Congress. And the third is way out there. We are to advise the President and other senior Executive Branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and policies dealing with the war on terror. That's a big job. The Board is not constituted, as some members of Congress had wanted and as some members of Congress currently think it should be. It had been proposed originally as an independent body with subpoena power. Somewhere during the legislative process, that was changed. We are now an office, as Hugo said, within the White House. I'm on the White House staff. We don't have subpoena power, partly because under the concept of a unified executive you don't need subpoena power to get what you need from other officers of the President. It was a trade-off that the legislative process made, and time will tell whether it works. We

don't have subpoena power, and I don't have an independent base from which to ask, but I do have a position, the Board has a position within the White House that I think gives it the gravitas necessary to make this work. And as I said, time will tell, but I'm optimistic at this point. We have spent the first six months of our existence learning, learning the players, learning the issues, trying to figure out where the Board can bring the most value. Because the mission is so broad, we can't possibly be everywhere and do everything, so it's going to be very important that the Board set its priorities. I have no doubts that, in time, we'll be criticized for what priorities we set. But, within the priorities that have been set, I hope we'll be judged by what we accomplish.

The Board has made a couple of very broad decisions at this point, nothing specific, but they've decided that they want to focus on those issues which have the most impact on the American public. The Board has decided it probably, at this point, is not going to get involved, although I think it has the authority if it wanted to exercise it, in the uniform war on terrorists. In other words, we won't be dealing with issues specifically related to Afghanistan and Iraq and military missions and what have you. There are a couple of very specific issues that we've gotten involved in that are important to the Board because they're important to the Administration as a whole. One is, it's kind of interesting. I'll talk about this in a minute. But as we've been reaching out to various individuals and organizations to get their ideas, one or two issues pop up uniformly. And the thought was, well, let's look at that because if you've got left, right, and center all suggesting that the Board get involved in a particular issue, there's probably good reason. One of it is the various watch lists and redress mechanisms. And the Administration has been working on this for a while, but it's a complicated task. It involves quite a few government entities. And the Board has been pleased to get involved and provide a level of support that lets everyone know that this is a major initiative of importance to the White House, to the Administration, and we'll continue to do that until we've got something that works for each of the agencies and for the American public.

We our spending some time getting up to speed on issues associated with, and I'm going to use this term very broadly and very loosely, data mining, because data mining means almost anything to anybody, and, quite frankly, it's become pejorative in most people's thinking. What I mean by it broadly is sort of data collection, data management, data use, data dissemination, and data protection. And if you define it like that, it pretty much encounters almost any policy on the war on terror. And, what the Board would like to do is become subject matter experts on all things data management, so that when programs and policies are thought about, when they're designed, when they're implemented, and when they're operated, the Board will be able to understand how the data management elements are working and be able to either express concerns to the appropriate individuals or be able to go the American public and say, "We've looked at this, we understand it, and this is why the American public shouldn't be concerned."

Now, I don't have any specific examples at this point, obviously. That's just sort of the philosophical theory that they want to pursue in that area. We have done our due diligence. The first thing was to reach out to colleagues within the White House staff. The Board has met. In fact, its first meeting was with then Chief of Staff Andrew Card, who subsequently met with Chief of Staff Josh Bolten. We work very closely with Steve Hadley and the staff at the National Security Counsel and Fran Townsend and the staff at the Homeland Security Counsel, and also with Harriet Myers and her folks in White House Counsel Office. Those are the folks I deal with on a day-to-day basis, and I can say that it's probably no secret that the Administration wasn't enthusiastically supportive of this particular Board during the legislative process. The thought was the President takes an oath to preserve, protect, and defend the Constitution, every member of his Administration does so, and every civil servant does so. The Department of Justice is there to guarantee that that's going on. The thought was why do you need five more people looking into these kinds of issues. But since the Board has been stood up, I can tell you I'm extremely pleased and the members of my board are extremely pleased with the amount of cooperation we've been getting from the people we need to work with. The thought is we're here, it's a very energetic group of individuals, and they should be used. So they don't set our agenda, but we've been working with them to find out if there are areas that we can bring particular value and things that they're already doing.

Interestingly enough, some of the issues that they had suggested, both the Homeland the National Security Counsel staffs, are issues that, again, some of the NGOs have talked to us about. So there is a clear understanding, I think, out there of the kinds of things that the Board can look at and bring value to. We've reached out to those agencies within the Executive Branch we think we'll be working with closely. Obviously, the Department of Homeland Security is one of them. I'm very pleased to have Hugo join us in this effort. I'm also working with Dan Sutherland and his staff in the Civil Rights and Civil Liberties Office. We've been working with Jane Horvath at the Department of Justice and with Alex, Joel, and his staff in the Office of the Director of National Intelligence. Those are the key agencies I'll be working with. And on any given issue, there probably will be others that we'll need to reach out to. Treasury and State come to mind, for instance. The Board views itself not as an institution standing alone. It's very important to remember that we're a part now of a structure that's being built. It's a structure that includes you all dealing with privacy and civil liberties. The Board is just one element, and it seems itself working very closely with our colleagues and counterparts throughout the Executive Branch. And I think we can help each other. One of the things that I've talked to Hugo and to Jane and Alex about is- we're here to help them. If there are issues that they need us to sort of shine light on to make their jobs easier, we'll do that. I hope that I can count on them as sort of early-warning systems. I'm in the process of building a staff, and we've got the ability to bring on detailees. But I

need their eyes and their ears at the level they work at. When programs are being developed, to have them developed and then land on my members' desks three days before they go to the President, there's not a whole lot of value we're going to bring to that process. What I need to do is have my staff sitting in on the early stages of policy development so that we can figure out what's going on and take a look periodically through that process so that when the program is done, at least ready to go the President, we know what we're looking at.

Let me talk just a little bit about staffing because I think Congress probably stumbled into it, but I think they got it right. I'm going to have a small permanent staff, but the statute allows me to detail in Executive Branch employees without regard to the existing six-month cap. Usually, when the White House details employees in, they have to, at six months, either send them back to their host agencies or reimburse the host agencies for their salary. I don't have to do that, and I'm the envy of my colleagues at the White House. So in designing a staff and meeting the needs of the Board, there were two professional types I figured I would need. There are attorneys and technocrats who understand the constitutional issues involved. And then there are the intelligence individuals who understand how programs work: operators, analysis folks. And in dealing with the intelligence community early on, I realized that, because we're a White House office, my position is political. I don't mean partisan. Our board is not a partisan board. But I will go when this president goes, regardless of what party takes the White House in 2008. It was difficult to go to the intelligence community where most of the employees are career staff and try and get individuals to come into the White House because they would be giving up their career civil service positions for something that is inherently short term. So what I'm going to be able to do is I'm going to be able to detail in those folks, and that allows me a little bit flexibility. Once the Board begins to set its specific priorities in terms of programs, I'll be able to cherry pick individuals with backgrounds that match those issues. I'm being aided by John Negroponte and his staff. I'm very pleased with the fact that they have made this a priority. He, in the process of trying to unify the intelligence community, has decided to do what the military has been doing, which is requiring a joint billing assignment of intelligence officers in order to progress up the professional ladder. He has determined that an assignment with our board will fulfill that element in a career development. We're going to bring in three initially. He's also going to pay for one of those three, and he's not telling the agencies which one. It's sort of a lottery, which will encourage, we hope, the agency's to put forward candidates. And they're in the process of doing that, and I can say from the resumes I've seen to date, I'm very pleased with the caliber of folks that are interested in working for the Board. One of the other things this joint billing assignment does, hopefully, having been a general counsel, having worked in the federal government before, I know that detailee assignments can be very valuable to the host agency, too,

because you can get rid of dead wood, someone you don't need, someone you don't want, and send them off for 6 to 12 months, and we'll try and figure out what to do with them in the interim. I think the focus that DNI is putting on this will prevent that. And, certainly, if I find that that's happening, I've got the ability to just get rid of these folks. The term of the detail will be for a year, but I'm not bound to keep these folks for a year. So I very much appreciate this word I'm getting from John Negroponte and his staff. We have been reaching out to non- governmental organizations, those who have a history of interest with privacy and civil liberties.

Clearly, the main folks and people we've talked with early on were the ACLU. We've spoken with the American Conservative Union, the Markle Foundation, the Center for Democracy and Technology. All of those entities which have an interest, that's intended to be an ongoing dialogue. We need to know what's being thought about out there in the community. I've spent an awful lot of time reading the work product of those organizations and others so that I, myself, have an understanding of what the current line of thought is. We've been able to bring some of those folks in formally. I've been able to touch base informally with staff with other organizations. And we intend to continue doing this, as the Board continues to fulfill its mission. We need to reach out to Congress. Interestingly enough, there was, early on, a lot of comparison with the President's Foreign Intelligence Advisory Board. That comparison between PFIAB and my board is helpful only so far. They have a constituency of one, it's the President, as do we. The problem is we had a chair and a vice chair confirmed by the Senate, and when you have that happen you have an obligation to go back to the Senate and the House when they have a reasonable request. So whereas members of PFIAB don't have any kind of formal ties with Congress, we do. And I've reached out to the appropriate staff, and we've been anxious to get the principals together, members of the House and Senate, with my board. Schedules have been such, mostly on the House and Senate side, that that has not yet happened after the actual confirmation process itself. But it's a busy season for them right now, so I assume that there will be more interest when the new Congress convenes in January. The Board has had, in six months, 12 full meetings, which is actually phenomenal when you think about it. I've got a chairman coming from Houston, and Frank is based in Connecticut. We have had very productive teleconferences. You know, going back to what I said earlier about the Board getting along with each other, I've had meetings before, both in the private sector and the public sector, where a group of people who can work very well together in person, it falls apart when you try and get them together on the phone, and that doesn't happen here. So given the geographical distance and the time differences and what have you, being able to put telephone conferences together is a great tool for me. We've got an office space. Since 9/11, White House staff no longer is solely based in the Eisenhower Executive Office Building. I'm actually at the 1724 F Street building. It's the old OSS building. It's actually a charming building, about

100 years old, and it's about 50 yards from the OEOB, so I can come and go as I need to. We've got SCIF space, secure space, so that we can get the briefings we need in our offices. And all of our members and staff have the highest level security clearance so that we can be compartmentalized or cleared into whatever program we deem important enough to do so. We've got a web page, for those of you taking notes, www.privacyboard.gov. That will be our primary means of communication with the public. We are not set up to do casework. I can't dedicate time and staff to individual problems. We're a policy tool here. But, nonetheless, we do get those kinds of complaints, and one of the things we do is refer it and try and determine where that complaint needs to go to be looked into. And it's interesting. You know, we get our share of -- you know, my son is stopped all the time when we go to the airport, too. I've got black helicopters following me and the aliens, so we're dealing with a broad spectrum of concerns and interests. I want to re-emphasize something that Ted Olson emphasized on the Ted Koppel Discovery special the Sunday before 9/11 last week, two weeks ago. And something that Hugo and our colleagues have discussed on a number of occasions and something that is very much the design of this administration, there are a lot of very, very important, very intelligent, very dedicated individuals now looking at issues of privacy and civil liberties, and you all are just one example of that. It is an ever-evolving activity, when you think about it. It's relatively new, even though the constitutional concepts are as old as the Republic, the actual mechanics within the Executive Branch are relatively new. It's going to take time to make sure everything is working. But the Board wasn't created in a vacuum, and we understand that. And what we want to do is reach out to the existing structures and make them better, work with the existing structures, work with Hugo, work with you folks. And to the extent you all have recommendations, ideas, interests that you think the Board should be pursuing, I'd be very grateful to know them. And if any of you have an interest in meeting with me and the staff personally or the members of the Board, let me know, and I'd be more than happy to facilitate that. And with that, that's pretty much where we are, where we're going. I'll be happy to take any questions.

CHAIRMAN BEALES: Mark, thank you very much for being with us today. This is very interesting. If the members of the Committee would follow our custom of turning up your tents and those of you at the ends of the long table can sort of push them to the middle so that I can actually see them, that would be helpful. Ramon?

COMMITTEE MEMBER BARQUIN: Thank you, Mark. I appreciated those remarks. Aside from the web site, how do you expect the work of the Board to get out?

MR. ROBBINS: That's actually a very good question. You know, I'm a litigator, I'm a lawyer. I like big victories and front-page notoriety when I win. When I lose, I don't like that. But this is the kind of job where our victories are going to be quiet. You know, it's very difficult to document the concerns you expressed at the policy-development stage,

the fine-tuning you recommended at the implementation stage, the comments you pass on at the program operational level. There will be pressers. There's been press. Usually, press is most interested when there's bad news, as I mentioned a little earlier. But I think it's the intent of the Board to do what it can without a lot of sound and fury. There is an unfortunate philosophy in this town that if you're not making noise, if you're not noticed, you're not doing your job, and I reject that. My colleagues at OPM, when I left to take this job, joked about, "Wow, now we're going to see you in the paper a lot," and I said, "Not if I'm doing my job right." So I don't anticipate that. I'm hoping desperately that we don't have a lot of notoriety. If the Administration deems it important enough, if we've done one thing in particular, then hopefully we'll get due credit. You know, some of the things we'll do will be public. Our involvement with the watch list redress process is relatively public. When that's ready to be rolled out, I hope that there's some good news, and I hope that the press will pick up on it and disseminate it to the public.

CHAIRMAN BEALES: Having spent some time in OMB doing regulatory review, I can appreciate the importance of quiet successes. Lance Hoffman?

COMMITTEE MEMBER HOFFMAN: Thank you. I'm very much sympathetic to your discussion about early warning systems. I think it's extremely important. One thing I've noticed in serving on this board and in other places is that, often, a bottom-up approach to programs. A lot of government programs, they start out, people have a good idea. They start the program. By the time the program gets going, it picks up steam, and it's too late to build up an effective privacy controls at that point. So I'm wondering, especially with regard to your priorities, watch list, redress, data mining, and that sort of thing, are there any ways you've been looking at potentially addressing early on, very early on, the privacy requirements? Because as a technologist, I know once you build things into the system, even forget the politics, once you build things into the system it's very hard to retrofit them and change them later. I commend to your attention there was, I believe at NIH, maybe it still exists there, where there's a certain small amount, percentage, I think, set aside in the RFPs, the grant process, the procurement process, somewhere, where you must look at this and don't even come to us before you've looked at this and this and this. I'd be interested in your comments or thoughts on this problem.

MR. ROBBINS: A good deal of time has been spent both by the members and by me and my staff with regard to inserting the Board into the existing processes that exist for policy development, which will go a long way toward achieving an early-warning system. As I said earlier, if we're not involved early on, it's rather difficult to accomplish our mission. You know, the various privacy and civil liberties offices are going about this differently, depending on how established the host agency itself is. They've established this brand new board within the White House. Well, the White House operation, you know, this Administration is six years old, and the White House operation itself goes back

decades to World War II really, as it's currently constructed. It's a new group of people being asserted into existing processes, and that's not difficult, and I'm getting the support I need. But it's one of those things where how do you know what you don't know? Well, you know, two people go off, and they're thinking about potential policy. Invite me, invite the Board. How do you know that's happening or not happening? So we're spending time making sure that we are fully integrated into those processes. Someone, you know, Jane Horvath at Justice is dealing with the same kinds of issues: a relatively new office in an existing structure. Alex Joel is creating his office within a new enterprise, within the new Director of National Intelligence. Hugo and Dan are sort of somewhere in the middle. The Department of Homeland Security is relatively new, but it was built out of existing component parts. So I'm hoping, and I'm probably going to have to fine-tune this as we move along, that integrating the Board into processes and procedures will accomplish an effective early-warning system.

CHAIRMAN BEALES: Joe Alhadeff?

COMMITTEE MEMBER ALHADEFF: Thank you. And I join the others in thanking you for the comments. They were very useful. And I guess I would build on Lance's point and maybe take slight issue with your last statement. And the issue being I think where you can insert yourself into the process, you clearly will make a difference. But the reality is that a board a five people and the processes of this government can never mesh because there's just not enough of you to go around. So I think the concept comes back to stuff that's been done, for instance, in the Privacy Office at DHS, which is the concept of let's create a PIA framework. In your case, it may be a policy privacy analysis versus an impact analysis that was related to systems or procurements. But I think there needs to be a concept of a framework. You were talking about developing expertise in kind of the data management elements as they come along, and I think that's a great objective for the group, but the group also has to disseminate that knowledge so that people who are actually developing the concepts because by the time the concept is reduced to a project and the project is already on its way to technology, it's too late to have an impact on it, which means inserting yourself in the process is great where you can, but where you can't you need to insert the information into the process and create a framework. And I guess to that extent, I would also recommend the fact that this group put out a framework document that might be at least an interesting construct to look at some of those issues. But I was wondering if you had any concepts of how you were thinking about putting things in the process. Because I think most people are well-intentioned as they develop their projects, but their job isn't privacy. Privacy is an element they're looking at, and, in many cases, they don't know how to frame that inquisition and they don't know how to frame the work that needs to come out of that.

MR. ROBBINS: First, allow me to thank you for the opportunity to thank this group for a lot of your work product. In fact, it has been very helpful in terms of building a sort of an analytical methodology and a process by which we'll be reviewing various issues that obviously have to be tinkered with, depending on what the particular issue is. But I have been spending a lot of time looking at some of the work product that's either come from or through this particular group. Your point is well taken. It's at the top of my mind. You know, Hugo, again, said it best: privacy isn't something you look at once. And the earlier you get into the process the more value you're going to bring, and one of the things I've got to do is identify opportunities and mechanisms both in which the Board can be brought into those processes. You know, when you're new you struggle with the issue of how do you know what you don't know, and I can't answer that question. I have to rely a little bit on the good faith of the people I'm working with and, when there are slip-ups, remind them, either gently or rather dramatically, that they had slipped up and that we need to be included. And I've had opportunities to do both, to say, "Hey, I hear you had a meeting. Could I come to the next one?" "Oh, yes, I'm sorry. We forgot all about you." That's not malice, but it's just as harmful to the policy-development process. And I'll say that as time goes on that's happening less and less. I'm never going to know what I don't know. My hope is is that as the Board begins to get its work product, whatever that may be, whether it's advice or reports or whatever, into the system and build relationships with the people who are designing and implementing policy, that trust will be there. It will just sort of be a part of the process. It's like, "We've got to get the Privacy Board into this." Again, as with everything else I'm doing, time will tell whether that's successful. You know, if I come back in a year, I'll be able to tell you where things aren't working and where they are.

CHAIRMAN BEALES: John Sabo?

COMMITTEE MEMBER SABO: DHS, through the National Infrastructure Protection Plan and the National Response Plan, and these other large national planning documents, is doing a lot of work to develop, in effect, a very large information-sharing environment with the private sector, with the critical infrastructures, with industry, with the responders, with states. And in the process of doing that, you're kind of seeing the boundaries of the outputs or the analysis of the national security community interface with the non-classified world, and you're dealing with sensitive but unclassified information. And those boundaries are clearly, the national security boundaries are very tightly constrained, but the need for the information pushes beyond those membranes and to the power companies and to IT companies and so on, through I-SAC, and through other mechanisms. The question is for your charge as a board with respect to reviewing the information-sharing environment, are you looking beyond the classified community for this and some of the implications for information sharing? And if so, you know, are

you planning to work through some of the initiatives that DHS or the private sector has in place to address that? I guess I'm looking for your sense of the boundaries of your charge.

MR. ROBBINS: Let me answer in a general way. And this goes back broadly to the Board's interest in data mining, data management issues. Yes, we are looking at commercial applications and the interaction between not only national security and non-security issues but commercial and public sectors. The Board's charge, while broad, statutory charge, while broad, requires there be a nexus on the war on terror. So our interest right now with non-security and with commercial data practices is mostly to learn how it's done in different sectors. You're going to be addressed later by Jennifer Barrett with Acxiom. She actually was before the Board at one of its meetings a few weeks ago, one that Mary was also at. Whether we'll be looking at specific programs or not, I obviously can't say right now. I will say one of the philosophical issues we're dealing with right now is, you know, we've got a role for both advice and oversight, which we're going to have to balance. I see advice coming mostly, not exclusively, but mostly in the policy development stage. Oversight will come in the program, operational stage. But does the Board want to look backwards? How much value do we bring looking at existing programs if there are structures already in place at the host agency to do that? We may bring value and we may decide we want to do that, but I don't know. That's one of the questions we'd have to ask versus prospective policy development. I don't know, but that's one of the things that we're focusing on now.

CHAIRMAN BEALES: Richard Purcell?

COMMITTEE MEMBER PURCELL: Thank you, Harry. Mark, one of the great complexities, one of the many great complexities of a data management program that attempts to ensure data protection and privacy to individuals is wrapped up in the whole idea of identify management. And it's one of those conundrums where the better we can identify an individual, the more we're able to, one, assure the individual certain protections. But at the same time, it's a lever by which those protections may be eroded, as well. And because of the ability to combine information under a single known identify, where that may be useful, it may not be useful, it may be purposeful, it may be harmful. There's a huge potential for misuse, abuse, but also a large potential for clarity, for data integrity, as well. So it's one of these knife edges that we all struggle with in data management issues when we're trying to provide a framework, a policy framework. So do you have or are you taking a particular approach to the various identity management schemas that are being proposed at the federal level, at the local level, through immigration, through driver's licenses, through commercial transactions, the raft of different proposals and solutions that are out there?

MR. ROBBINS: Very simply, not yet. We're not anywhere near that level yet. We literally are still reaching out to the various sectors that we think will bring some valuable

information and so that the board members can get that key base of knowledge before we get to that level but certainly we will; yes.

CHAIRMAN BEALES: Ana?

COMMITTEE MEMBER ANTON: Thank you, Mr. Robbins. I have a question regarding the ISE, which you mentioned. You said that the Board's mission, one of the Board's mission was the development and implementation and guidelines for the ISE. And as you well know, this a huge systems engineering challenge. And so my question is how is the development of ISE being managed, and what is your relationship with that development team? And when should we expect for this to be fully operational?

MR. ROBBINS: Well, I'm not going to answer specifically that question when it's going to be fully operational. The process itself began before the Board was sworn in. There are five sets of guidelines which will eventually be released, and the one of particular concern to our Board, we're concerned with all five, but the fifth set, which is being managed, the working group is being managed by both DNI and DOJ, deals with privacy and civil liberties. And it sort of cuts across all the other guidelines, making sure that there are processes and procedures in place so that privacy issues are being adequately considered and discussed. There are working groups. Each of those five guidelines are chaired by various departments and agencies, specific agencies. The Board and the Homeland Security Counsel and the National Security Counsel staff are sort of spearheading and coordinating the efforts of these organizations and bringing them together periodically for status conferences. I attended the first meeting probably about two months ago, the first general meeting. Alex Joel and Jane Horvath have kept the Board briefed in great detail on the fifth set of guidelines, the ones dealing with privacy and civil liberties. And I'm actually quite pleased to say that that is, the first set of guidelines that was sort of put on the shelf and ready to be rolled when the rest of them are, we're done with that, and we're now waiting for some of the others to catch up with us. It's difficult to be inserted into a process that's already begun, as I said earlier. I think the Board thinks, the Board believes that it will bring most value to the information-sharing environment in these guidelines in its oversight role because we weren't around at the very beginning when the concepts were being developed. So out of necessity, we're going to have to focus on the stand- up processes and the various operational elements of the guidelines. Now, one of the issues we're contemplating and I'm working with White House staff on is what mechanisms do we need to develop and how regular do those mechanisms need to be invoked in order for the Board to get the information necessary to make an assessment on whether these guidelines are being followed generally and whether they're working as designed. We won't be alone. I mean, the departments and agencies working on these guidelines will be part of that process, too. But it's going to be very important for the Board, and not only the Board but, frankly, for all the Executive

Branch to understand what the responsibilities are in reporting back to the Board so that we can do our job. And that's where we're focusing our energies right now.

CHAIRMAN BEALES: Well, Mark, I want to thank you very much for being with us. This is certainly a group that's very interested in what you're doing and in your mission. I think there's, we are also thinking about a number of the issues that are on your list, including redress and data mining kinds of issues, as you find it. And we'd like to do anything we can to help you out. Consistent with our mission with the Department and the Privacy Office, we'd like to do anything we can to help you out and facilitate your job because it certainly is a challenging one.

MR. ROBBINS: Thank you. I appreciate this opportunity and, again, if anybody wants to contact me directly, you can either do it through our web page or through Hugo and his staff.

CHAIRMAN BEALES: Thank you very much. Our next speaker is Tamara Miller, the Special Counselor to the Assistant Secretary and the Deputy Assistant Secretary at the Transportation Security Administration. Ms. Miller oversees the work of several TSA offices, including Executive Secretariat, the Audit Liaison Office, the Freedom of Information Act Office, the Sensitive Security Information Office, the Office of Civil Rights and Liberties, the Office of the Ombudsman, the Privacy Office, and the Office of Transportation Security Redress. Quite a portfolio. In her previous position, Ms. Miller was the Director of Civil Rights for TSA and was the Senior Technical Expert for the agency in all matters involving civil rights and civil liberties. Prior to joining TSA in August of 2003, she was the Deputy Chief and Trial Attorney in the Civil Rights Division in the criminal section of the Department of Justice for seven years. Ms. Miller, thank you for being with us, and welcome.

MS. MILLER: First of all, let me welcome all of you to the Transportation Security Administration. I do believe this is the first time this committee has walked these halls in this important session, so thank you very much for being here and allowing us to host you. Last week, we celebrated, as you all know, a very macabre fifth anniversary. All of our staffs were out in the courtyard here reflecting, reflecting. And as I was thinking about my comments today, I thought it might help you in terms of how we think about privacy and where we've come to sort of set that stage for you. Two months after 9/11, on November the 19th, 2001, Congress signed into law the Aviation and Transportation Security Act, as you all know, ATSA. That statute established TSA. So in just a short two months, we will, in fact, celebrate our fifth anniversary. We received some 33 mandates from Congress in that legislation, as you all might remember. Perhaps the most significant of which was to hire, train, and deploy some 55,000 screeners at over 450 airports in this nation. And to do that, in six months. Phenomenal. Never done before. And, certainly, we had some hiccups along the way, but I'll tell you, five years later -- oh, the other thing,

from a privacy perspective, we had some 1.3 million applications for those 55,000 positions. What does that tell you? Our nation answered the call. We had people who wanted to work in this agency, and I can tell you today that that mission call is still strong. You can look back at August the 10th and those terrorist threats from the UK and know that this mission is still vital today. So, five years later, it's my privilege to address to you on this topic that is near and dear to Assistant Secretary Hawley, the head of our agency: the Privacy Office at TSA and how this important mission is supported and interwoven into the fabric of this agency and supported in my office.

The Office of the Special Counselor was established in October of 2005. Kip Hawley asked me to pull together several offices at TSA whose functions were to support the entire agency. I call all our offices agency programs because we ensure that employees in the traveling public, this is lip service, we ensure everyday that the employees and the traveling public are treated in a fair and a lawful manner consistent with federal laws and regulations protecting privacy, affording redress, and prohibiting discrimination and reprisal. I attended some of Kip Hawley's very first town halls in the August - September time frame in August of '06, and I was struck, I think most of us were struck by a very bold statement that he made and, frankly, that he repeated at the PIA conference that was hosted by the DHS Privacy Office this past June. Some of you may have been there. I just thought I would give you an employee's perspective on that. When Kip Hawley told us, "Here's the thing. I'm going to do a lot of things in this agency that are, hopefully, going to improve us, improve our processes, and our mission effectiveness." But what he said is, "We need to rethink how we approach privacy and civil liberties." He told us all that. And, to demonstrate his thinking on that, he said, "Let's evaluate how most people think of privacy."

Most people, including TSA at the time, thought, well, let's build these programs. We have lots of important programs, lots of them: Secure Flight, Registered Traveler, Transportation Workers Identification Credential Program, and then on and on. We build these programs typically, and then we think, "All right. Now, how do we make sure, from a privacy perspective, that they're sound?" He said, "Let's flipflop that analogy and let's start first thinking about privacy and civil liberties in this agency and in this country because the reality is we can't do this mission unless we put those things first and build the programs on top of them." Ladies and gentlemen, I'll tell you that I hadn't ever heard that before, and that radical thinking has influenced me, as he's asked me to help him achieve that vision. So what have we done? This past year, we have, we've done lots of things. I've added personnel, most notably Peter Pietra. Mr. Pietra is a skilled attorney, expert in privacy law, but, most importantly, a visionary. He's a guy that I recruited to come over from the Counsel's Office where he was providing advice and charged him with the responsibility of building a program. What's he done? He's brought on additional staff. We've changed the name of the office from the Privacy Office to Privacy

Policy and Compliance because, in my view -- I'm a lawyer, as you know -- in my view, it's not just what you tell people you're going to do up-front, it's how you evaluate their compliance. So just to show you how serious about that that I was, we changed the name of the office to include that important compliance role in its title. And we really wanted to capture both privacy issues in the news and, of course, the nuts and bolts of our daily operations. So what does this mean? I just thought I'd give you some examples. I know that you will have other people to tell you more in detail. But what we do is we use privacy impact assessments to shape programs. It's a wonderful tool, as you well know. But we want to shape their collection, their retention, their sharing policies, and we want to make sure to follow up with them to make sure that they're complying. We do this with constant interaction with the programs.

Folks, as we move forward on Secure Flight, when Mr. Hawley addressed this PIA conference in June, he spoke a lot about Secure Flight, but I'll tell you it's not just about Secure Flight. Mr. Peter Pietra and his team is moving forward working with these programs. We're talking rolling up our sleeves at the meetings with the people as they are designing, even conceiving, their programs. On Secure Flight, we worked very, very closely with that team; Registered Traveler, as I mentioned before, Redress. You'll hear from Jim Kelly, one of my managers. He provides critical advice on our Redress Program, the Hotel Guest Program, and others. We are doing lots of things at the boots level, where the rubber meets the road, to ensure that we ask these program managers what information that's personal information, what PII do you want to collect, and does it make sense from both a security and a privacy standpoint? If we do that at the program design and development point, I know you all know we'll get good results. We've also instituted a privacy system review where we systematically, sometimes with notice and sometimes on an unscheduled basis, look at programs to evaluate their PIAs and so on, to make sure that they're accurate, they're up-to-date, and they reflect the current program goals and realities. Mr. Pietra, although he reports directly to me, I want you to know he has direct access to Kip Hawley. He attends our weekly leadership meetings. He sends out broadcast messages on privacy training initiatives, and he's been working on building those existing and very good relationships with our chief counsel and with the program offices and field contacts. It also means raising the profile of privacy within TSA so that it becomes second nature for those programs to consult with us. We can't just sit in our office and wait for that program to say, "Oh, I've got something I want to run by you." No. Peter and his team, we know where the programs are. We know they're all requiring federal register notices. We know where those are. We proactively go out and meet with these teams at their meetings, talk with their staffs daily. And we want to do that so that way these folks are trained to consult with us at the early stages. How else? It means that we need to develop policies to reduce the potential for the types of privacy breaches affecting government and the private industry that we've seen all too much recently. But,

you know, it also means thinking outside of the box. I'm going to give you a little tidbit. Peter Pietra is doing something that, to our knowledge, hasn't been done. I mentioned to you that we had some 1.3 applications for 55,000 jobs, and we had to fill these jobs within six months. The only way we did that was to partner effectively with industry. And you all know lots of our work is supported by private industry because we out-source so much of our services, including human capital services. Well, we think how do we really get at making sure that not only our employees understand privacy but that our contractors understand it? So what Peter Pietra is doing right now is he is using and working with our acquisitions office to use that request for proposal process. Many of you have been in the federal government and you know how it works. Use that process, evaluate what these vendors tell us because, of course, they all have to give us a privacy statement. Well, that's a piece of paper with letters on it and words on it. We are asking what their experiences are with protecting privacy, and we want to make sure that the contractors, and we are evaluating new contracts everyday, that those people really know and value privacy and how to secure very vital personal data. And, of course, last but not least, privacy at TSA also means close interaction with the Department's Office of Privacy. In closing, this committee should feel confident that privacy, civil rights and liberties, and redress are in capable, motivated, and dedicated hands at TSA, well-supported by Assistant Secretary Kip Hawley, by his special counselor, and her office. Questions?

CHAIRMAN BEALES: Thank you very much for being with us today. Secure Flight, in particular, is one of your programs that we've been very interested in and this committee has had something to say about. I'm sure we do have questions. Lisa Sotto?

VICE CHAIR SOTTO: Thank you. Thank you so much for testifying. And I am very appreciative of the forcefulness, I think, that you bring to the job. We are really looking to you for help for the TSA in this arena and to Peter. And we're delighted, I'm delighted to hear all that you're doing, and it sounds like you've got a great framework set up in moving forward. So congratulations for doing that, and we'd love to hear follow through as you move forward. My specific question, with respect to contractors, do you require that they do ongoing training, periodic training of their folks with respect to privacy? And do you do ongoing monitoring? And I know that's difficult and it may be that you're just setting that up right now, but you talked about building privacy into the RFP stage, which is fabulous, and Jen may want to address that, as well, because her subcommittee and Jim's subcommittee are thinking about building privacy into that RFP stage. So in addition to that, I would just say that that doesn't really seem to be the get-out-of-jail-free card. I think ongoing monitoring is really essential, as well, as well as continuous periodic training in privacy.

MS. MILLER: This is absolutely an initiative for us, and we're excited that our acquisitions office embraces this. The other thing I'd like to share with you is that part of

this partnership with the Department is to help us leverage their training initiatives. As you know, this department's privacy office is really helping to lead the Department in terms of setting the standard for training. And through close collaboration, I can assure you that we will be working with them to develop just those kinds of rigorous ongoing evaluative on-the-job day-to-day training initiatives. So we're excited about the potential. And I'll tell you that we're happy to have any advice that we can get. Peter will be here all day, and I know he'll be anxious to talk with you about this initiative. Because as far as we know, it's something that hasn't been done typically in this new arena. Thank you.

CHAIRMAN BEALES: Joanne McNabb?

COMMITTEE MEMBER MCNABB: Thank you. A couple of questions. As Lisa said, we have been interested in the Department's acquisitions process and how it might be possible to build privacy considerations early. And I wonder if you can give us some documentation of the process you go through or somebody we can talk to about the process?

MS. MILLER: Well, absolutely. Peter Pietra is working now with our acquisitions office. And as I said, he consults very closely with Mr. Hugo Teufel and his staff. So stay tuned. We will absolutely be able to share and, hopefully, consult with you on some of these initiatives.

COMMITTEE MEMBER MCNABB: And like a contact that we could talk to by phone in between meetings, as the subcommittee works on that issue?

MS. MILLER: Oh, absolutely. We'll work with Becky and the team and certainly make Mr. Pietra available to you.

COMMITTEE MEMBER MCNABB: And, also, are you doing a new PIA on Secure Flight?

MS. MILLER: Well, we are working closely with the Secure Flight team. I know that there will be, **I know that addressed you yesterday**, and so I don't want to comment very much on those specifics because I know that that work is ongoing. I will tell you that every PIA that's issued in this agency is a result of close collaboration between the program offices, Peter Pietra, and, of course, our Office of Chief Counsel.

COMMITTEE MEMBER MCNABB: And so does our subcommittee know more about a new PIA? Okay, good. Thanks. Thank you.

CHAIRMAN BEALES: Jim Harper?

COMMITTEE MEMBER HARPER: After our last meeting in San Francisco, I took a dare to fly without showing ID to the delight and consignment of my colleagues. It was a wonderful experience. But since then, I've heard from a lot of people who are doing so or trying to do so, and each seems to have a different experience with that. I'm just

wondering what you may have done to educate, I think, TSA employees about the fact that people currently have the option between showing ID at the airport and taking secondary search. I imagine people who show up at the airport not well dressed and not as polite as I was that morning get a different treatment than I did, and I think it's important that people know about the work you've done to educate the public about the fact that they have this option. What have you done up to this point?

MS. MILLER: We're certainly looking forward for other opportunities to train, and, certainly, that is something that we can take back and look at. But I want to share with you all that this process of checking and verifying identification is something that TSA is not solely responsible for, as I know you well know. This work is certainly influenced. The very first experience you ever have at the airport is with a ticket agent, an airline ticket agent. So what I will share with you is that part of the challenge here is training them, as well. Certainly, you know the rules that you can actually go to the airport currently without an identification document, and you would be subjected to enhanced scrutiny, enhanced screening before you get on a flight.

So one thing I think you will find very interesting that you'll hear from Mr. Kennedy is that we are thinking about how we can partner with private industry, in this particular case the airport industry and the airline associations, to help train them not only on privacy issues, identification issues, but also redress issues. And so I'm really pretty excited about an initiative that we've got going on now where we want to train ticket agents about what to say to people if they are watch listed or their flagged as a watch list item at the ticket counter. Because as you know, no matter how much work we do here, the traveler's experience is influenced so much by that ticket agent. And when the ticket agents tell folks that you're on a watch list, 90 percent of the time they're not. But certainly it upsets a lot of folks. So we're going to get at that by training and reaching out to the industry itself, and we've already done that. We've made some significant inroads, and we'll make that happen this year. To give them a script, you know, programmed information so that they don't tell people erroneously that they're on the watch list. We have names similar, perhaps, or the system can't distinguish them, but they're not, you know, 90 percent of the time they're not on the watch list, as you well know. Stay tuned, James.

CHAIRMAN BEALES: Joe Leo?

COMMITTEE MEMBER LEO: Thank you. First, I applaud your energy level for pursuing this topic with vigor and, from my personal perspective, you have a lot of work ahead of you, so you'll be gainfully employed. And the reason I say that is because of your earlier list and there are many more besides that of systems, of records that you have, and systems that you're operating, like TWIC and other systems. But I didn't hear the mention, it seemed to be it would be in your office, a more systemic, holistic view of

how the systems interact. And what I mean by that is that we're all aware that a system in itself can be reading all the PIA requirements for protecting privacy and civil liberties. But when you sit back and look at systems, holistically, in a way systematically interacting with each other, you find some interesting things. When they start connecting to other systems, to other systems, and they start pooling information and information sharing, you wind up with a whole potentially different picture. And so what I personally haven't seen yet is vision with regard to holistic examination of your collection of systems, and then what does that tell you? And so I'm asking that question is it where your office is located that would take on that holistic challenge of TSA's many systems, or is it somewhere else?

MS. MILLER: Our Office of Process and Technology headed by Assistant Administrator Randy Knoll is where our CIO, our Chief Information Officer, sits. And we have a very strong IT security office within the CIO's office whose job it is to do just that kind of systems review, C&A accreditation. In fact, our redress management system that we're going to hear about, you'll hear about later on today, went through that rigor. And so the Committee can certainly invite Mr. Knoll and certainly hear a lot more about just how much progress TSA has made this past year in particular that I know and the C&A review for IT security issues and making sure that that data is secure, no matter how it interfaces. And Mr. Knoll is also building our enterprise architecture because, as you all know, information sharing is not just a buzz word. We need to do it more effectively here with technologies that tie our airports -- as I said, we have some 450 or so airports out there that need to be tied with us, as well. So this is a monumental challenge that our CIO's office, I'm confident, is up to, and they're the people who can address that.

COMMITTEE MEMBER LEO: Well, may I follow up just a moment? I am familiar with, C&A has done several, and I'm familiar with all the other good stuff that the CIO's office does. But I want to just sort of ask, to drive this one step further in that they really have very little, if any, skills in looking at the privacy and protections. When you link the systems together and see what happens and then the analysis systemically about, "Hey, now that they're linked, we're in some kind of non-compliance of privacy and civil liberties protection when they're linked. When they're not linked, we're okay. But when we're linked," and that's what I'm driving at. And I'm coming as an old CIO myself, I know that -- I was a CIO in Agriculture a few years ago -- that the skill level necessary for that type of analysis really comes from offices such as yourself, etcetera.

MS. MILLER: Mr. Pietra is charged with continuing to build his office, and I will tell you that he and I are looking very, very carefully at this possibility of adding to the staff just such a person who brings that IT depth and who can help advise the CIO's office in those regards. So, trust me, we're building, and I know Mr. Peter Pietra is here today, so you can assure that he'll take that as a get back. But thank you. I know that we value

the work of this committee because it helps us get at those priorities. So, please, work with us.

SPONSOR TEUFEL: I just wanted to jump in to say that we work very closely with Peter, and he is a valued colleague of ours over at TSA. I think we've embarrassed him some.

CHAIRMAN BEALES: Well, Peter, we will certainly be talking to you. Neville Pattinson?

COMMITTEE MEMBER PATTINSON: Thank you, Mr. Chairman. Tamara, thank you. It's been very, very interesting. TSA is about to embark on issuing the first batch of TWIC cards. We've been looking at this for three years, and we're nearly upon us with the phase four under our feet right now. Could you give us some indication as to what protections are in place for protecting the privacy of the credentials of the port workers, how that's going to be procedures for adjudicating, their eligibility, and also the redress of those credentials?

MS. MILLER: Well, you're asking very technical questions that I'm certainly not the best person to answer. But I will tell you that Peter Pietra has worked very, very closely -- and his team by the way, he's not just a lone soldier. It would be too much work -- work very, very closely with the T- TAC program that you know is headed by Stephanie Rowe and the TWIC team there. So we've worked very, very closely with this team. So I know the documents will be out there for publication and review and comments, so just stay tuned. I think it wouldn't be appropriate for me to give you any more than that, and I certainly don't feel qualified to do that. But just know that amongst the programs that are our top priority are TWIC. And when Mr. Hawley says we build it first with privacy in mind, he really means that, and that's what we're doing.

CHAIRMAN BEALES: All right. Thank you very much, Ms. Miller. We really appreciate you being here. You are clearly very enthusiastic about what you're doing, and we appreciate that. We think it's important.

MS. MILLER: My managers are equally enthusiastic. Take care. Thank you.

CHAIRMAN BEALES: Our next speaker is Kathleen Kraninger, who is the Director of the Office of Screening Coordination. Previously, Ms. Kraninger was a professional staff member for Senator Susan Collins, the Chair of the Senate Homeland Security and Governmental Affairs Committee. And prior to that, she worked as a policy advisor to Secretary Ridge and also to Secretary Mineta. So welcome, Ms. Kraninger.

MS. KRANINGER: Thank you very much. I appreciate the opportunity to be here and meet with all of you. It's an extremely important mission that you have in contributing to what the Department is doing and trying to enhance our abilities in the proper manner to secure this nation. So I do appreciate that. I wanted to take the

opportunity this morning to do a few things. One is introduce myself to you. Looking around the room, I know some of the names, but I don't believe that I've had the opportunity to meet with any of you individually at length, and I wanted to open myself up to that. If there's anything that I say today that raises questions in your mind, or if there is further work that you're doing, both as the committee and subcommittee, but also in your own endeavors, I would be happy to open up that dialogue with you because I do respect and appreciate the inputs that you have, just given your professional background, and appreciate the time you put into this kind of effort. So thank you for that. I'll introduce the Screening Coordination Office that has been a long time coming and tell you a few things about what we are doing and ways that I think you can help. First, just about myself, you gave a very brief history, but at least I can say that I started out with this Administration at the Department of Transportation. And as many of you know, what happened with 9/11 dramatically changed what our perspective was and what we thought we were going to accomplish over, you know, the four years of the first part of this administration. So I would say I was very personally impacted by that, was at the Department on 9/11 when all of us were just taken aback by what had happened and really knew that this was going to change everything that we were doing moving forward, and it definitely did. You will hear from my boss shortly, I guess, the Deputy Secretary coming down, so he can talk very much about what he was doing at that time, as well. My involvement was more on the maritime security side initially, and then I moved to work for Secretary Mineta personally on TSA and aviation security and basically followed these issues, given a personal interest, over to Homeland Security. And that was, it's been a tremendous opportunity, both personally, on behalf of the country, and thinking about all of the people out there who really need what the Department stood up for. And, also, professionally, it's definitely an interesting area, as I know many of you feel the same way since you're here today. I had a slight detour going up to the Hill. I worked on the Homeland Security Committee. But as you know, too, the Homeland Security Committee has the historic governmental affairs responsibilities. So I actually was able to work more closely on privacy issues for Senator Collins. So it was also interesting. And Nuala O'Connor Kelly, too, just historically worked with her office quite a bit at DHS on many of the programs that you're spending a lot of time on, including Secure Flight and the Jet Blue investigation and many of the things that she had done. So I do have some history in those issues from the policy side. But just getting to what is the Screening Coordination Office, there is a bit of a history and some different expectations, given its first introduction in the President's FY 06 budget. So I wanted to tell you a little bit about how the scope of the office has been shaped and what's happened. I was appointed just six weeks ago to start this office. It was originally proposed in the President's FY 06 budget. It was proposed as actually a program management office to consolidate operationally and in terms of program management programs like Secure Flight and TWIC and the Registered Traveler/Trusted Traveler

programs at at CBP and TSA. And that original vision, obviously, did meet with some opposition on the Hill, in part because I think there were some concerns about each of these programs and the paths that they were on and how those programs would interact in a new office and, frankly, whether those programs would be delayed any further by bureaucratic changes and program changes. But I think, at heart, the purpose of the office was recognized as a real need. It was appropriated \$4 million in FY 06 to carry out the mission. And, I was appointed six weeks ago, and I'm really just getting the office stood up.

But the mission really, as I see it, is strengthening homeland security by enhancing the screening processes and technologies. I would offer kind of four key areas that this is happening. One is just designing a framework for screening, harmonizing the business processes across the screening programs, and I'll get into these in more detail; facilitating more efficient and meaningful information sharing; getting the right people the right information at the right time to make the operational decision that they're faced with. The next thing would be infusing transparency and enhancing privacy in these processes. And the fourth is enabling more effective investment decisions, rationalizing and prioritizing these investments, and looking across the screening portfolio. As you are very familiar, we have a number of programs across the Department that are engaged in various pieces of screening. And I think what this comes back to is the operational needs of the front-line employees of the Department, meaning you talked about TSA and, certainly, we want to make effective decisions about whether or not individuals are a threat to aviation and whether or not they should be able to board an airplane. You know, how do you make those decisions? What's the information that you can use to make those decisions? And CBP is the same issue. You know, whether this person is eligible for admissibility into the United States and the basis for those decisions.

It is coming up in a number of areas, too, with the employees of the Department and the employees across government. What kind of screening is happening regarding new hires, and related to many of those things is credentialing? Somewhat controversial in different contexts, but both mandatory programs and voluntary programs, how do we basically recognize a person that we have vetted? And oftentimes, it's in issuing them a card, and how that card is used, obviously, becomes a great concern to people and how their information is used related to both the vetting that was done and what is on the card and what the front-line employees know when someone presents themselves with one of these cards. So that pocket of issues there is what my office is really tasked with looking at. The other thing is, too, we've seen long histories on each of these programs, and some are off the ground and some still are not. And my job is to really bring the program perspective to a lot of the departmental decision-making. How does the TWIC program get better visibility into the privacy requirements, the investment-decision requirements, program decisions that are happening in other places across the Department, and how we

can just basically more efficiently operate as a department, and how we can leverage the other investments that are being made.

A few things that will at least help you maybe express this more clearly, just things that the office is looking at right now. One of great interest to you is redress, I know. We are tasked with the responsibility of carrying out the Rice-Chertoff Initiative Promise of one-stop redress. And I'm strongly supported in that effort by Hugo's office, as well as by Dan Sutherland and the U.S. Visit Office. So we're kind of jointly moving forward with the redress responsibility and pulling together each of the programs that is, you know, individually impacted by this. And as you have looked at it, there are a few things around the redress issue, largely, I guess, varying levels of sophistication I would say with each of the programs and each of the agencies. TSA, obviously, as Tamara mentioned and Jim Kennedy will talk a little bit more about, is ready to launch something that really is a dramatic improvement, and they've made many improvements, as you all know, over the past few years in dealing with, you know, the no-fly list, the selectee list, management, and redress. But we recognize that when you're talking about the terrorist watch list in a global generic sense, since we know that there are different parts of that; but, as we talk about that, that data is being used by CBP and TSA and other agencies. So when an individual is presenting themselves at the border for entering the United States, we have a little bit more information on them than TSA does when an individual is going to present themselves to board a domestic flight. Is there the opportunity within legal parameters to share information on an individual who is misidentified as someone on the watch list? And CBP, too, I'm not sure how familiar this group is with their process, but they've also instituted a process called PLOR, the Primary Look-Out Resolution, I think that's what the "R" is. At any rate, they are putting in redress actually into their operations to say this is a misidentified person. Well, how do we share that with TSA so that the same person doesn't get resolved by CBP, move into TSA's checkpoint, and go through secondary screening or other issues because TSA doesn't know that that person has been misidentified? So we are trying to share some of those things on the back end of redress. The Rice-Chertoff Initiative Promise, of course, was really about the public face, though. So how do we put a little more transparency into the public side of this and give the public one-stop redress. And we are working very carefully on those issues. I think there are complications, as you all know, in pulling that together, but the promise has been made, and it's important to show the American people that we're making progress on that and, frankly, to help welcome foreign travelers, which was the Rice-Chertoff Promise, as well, and the motivation is to give a little more transparency to them as they have many more complications in trying to understand what the United States' policies are. The second area, and it's, again, one of great interest, is Secure Flight, but it's not just Secure Flight. It's how does the Department of Homeland Security screen air passengers and air crew pre-departure? So this is bringing CBP and TSA together in a holistic sense really on

those two processes, and how do we vet those individuals, how do we do that in a more streamlined fashion, frankly, and get the same decision about a particular person? And we are making progress on that.

And credentialing I had mentioned a little bit earlier, and I will elaborate on that. There have been a number of public statements about the need for one card. You know, how many cards is the Department actually issuing for different programs? Are we encountering the same person? Are we treating the same person in different ways, depending on the program? And, clearly, within the legal authority that we have, what are our opportunities to make those more efficient? And we are looking at that. I think it's going to take time. It's a systematic thing that needs to happen that hasn't happened, but we're trying to take the business process and the business needs, and I think, Mr. Leo, this gets to the point you made a little earlier, let's look across those businesses, figure out what we need and why we need it, be more transparent about describing that to the public, and proceeding forward. When you're talking about tying systems together, it does get concerning. And it comes back to, from where I sit, it comes back to what do we need, what are we trying to access that data for, and let's talk about what those systems have to offer to improve each process and being transparent about that. So I think that's what we're trying to do with the credentialing initiative. There are processes that really are the same across programs, whether you take TWIC or whether you take the Western Hemisphere Travel Document or whether you take Registered Traveler or other trusted traveler programs, you have to enroll people, you have to identity-proof and vet them, you have to think about card correction and the type of card you're going to use, how it's going to be used, which there's some technology decisions in there, and what information is going to be on those cards or how it's accessed. All of those things are shared across these programs, and how do we make sense of that both from the investment side and from the privacy side to do our best to describe that to the public and make better decisions about our programs and how we move forward. I did start this discussion with just my offer to you to be available. I would like to take any of your comments and would like to discuss things that you see as priorities for this office, issues that you'd like to see us working on. As I noted, I've been on the job now for six weeks, so it's not a robust operation yet, but it's definitely something I'm passionate about, something that the secretary is passionate about, and we want to make some real improvements in the way that we operate over the coming years. And the last thing is a plea to you, too. We definitely need at the Department the kind of business technology experts who can solve some of these problems from the inside and are willing to come into the government to be part of these kinds of programs. I mean, that's something that I don't know if anyone has mentioned to you probably that directly before, but you have noticed some of the program management changes and the challenges that, you know, we've had getting some of these things off the ground. And in part, that's some lack of experience, some

lack of expertise within the government in some of these key areas. And so I would welcome you to, if there are people that you know that want to do that, if you yourselves are interested in doing that, giving up that big paycheck and coming over and working it from the inside, but we are looking for that. And I certainly welcome anyone who's interested in that to come and talk to me about it, too. And with that, I'm happy to take any questions.

CHAIRMAN BEALES: This is a group that's busy doing its work for the government for free.

MS. KRANINGER: Yes, that's true, too.

CHAIRMAN BEALES: Could you say a few more words about the Rice-Chertoff Initiative and just explain a little bit more what that is and how it fits with what you're doing?

MS. KRANINGER: Absolutely. Last January, Secretary Chertoff and Secretary Rice, mostly prompted by the travel industry, initiated what is across the spectrum kind of promises regarding how we would improve as a U.S. government our welcome to foreign visitors. And so there are a number of facets to that. I was not at the Department at the time, so I'm not really the right person to explain in full what the initiative is all about, but one of the promises was one-stop redress. And, of course, it's left to those of us who are implementing to figure out what that means, but the bottom line is just a public face, a better way for, again, particularly foreign travelers, but this clearly affects domestic travelers, as well, because they're many times the same person who is both coming into the country of CBP and connecting to a domestic flight and interaction with TSA that way and on their return. So how do we basically give them the opportunity to voice any complaints they've had when there's been a delay in their processing that they perceive as related particularly again to watch list checks and what kind of information they think or have been told by the airlines, as Tamara said so eloquently, you know, what do they perceive their problem to be and then how we can we actually give them redress, as in fix the issue. If they are a misidentification, let's make sure that DHS operations can flag that and, in the future, we can avoid the problems that those individuals have. So that is one of the promises. December 31st is actually the first, I guess, due date for a progress report on the initiative at large.

CHAIRMAN BEALES: All right. Thank you. Larry Ponemon?

COMMITTEE MEMBER PONEMON: Thank you, Mr. Chairman, and very nice hearing your comments. I appreciate it. I actually have one question, and, basically, if you think about screening and dealing with the false positive problem, and it's really important to make sure that you do that right, you might actually diminish, by focusing more on that you might actually diminish program effectiveness or efficiency. In other

words, the mission is to find the bad guy. I know you don't want to be wrestled to the ground, you know, at an airport and then find out later it's just an innocent person. But on the other hand, how do you actually build your process so you don't actually have too much transparency, thereby diminishing the effectiveness of the program? Are you considering that at all?

MS. KRANINGER: Absolutely. I mean, clearly, there are certain things that can't be released publicly, but I think it comes back to how do we, as a government, explain what it is that we are doing and why we are doing it. And I do think that the UK threat is a good example of improvements in how DHS communicates that to the public. I may be a little biased, but I certainly think the Secretary did a fantastic job with that and that Assistant Secretary Hawley did, as well, as we talked about liquids and what you could and could not carry on board and why that is. And, clearly, there are all kinds of things behind that decision that the public doesn't know about and shouldn't know about, in terms of what went into that. But in terms of describing it, that's the kind of transparency that I'm talking about, and I think that we owe that to the American people, frankly. And as Hugo said, though I didn't hear him, but I did hear that he did actually say what he had planned to. And this is not about a trade-off between security and privacy. I mean, that is not what this is about. Frankly, the two are intertwined here, and we can actually, with making smart choices, move the two forward together.

CHAIRMAN BEALES: Charles Palmer?

COMMITTEE MEMBER PALMER: Thank you. This has been very interesting. When a standard is put in place for an ID card for previously vetted individuals, such as you describe, and it sounds like a wonderful idea. Of course, that target, the target now becomes the card and can the bad guys beat up on the card? Some of us have experienced assessing the security of these cards and the protocols and the standards around them because without strong security there's no point to even try to get data integrity and privacy. Some of the standards proposed thus far have been, well, disappointing from a security point of view. Knowing what high assurance technologies are available, we've been disappointed. That's why we've been disappointed. You mentioned this one card, and this sounds like a glorious opportunity, as so many of your colleagues have been saying, to get it right the first time. Is there any plan or hope for a plan to ensure that these cards do embrace modern technology, both from this country and others -- I know that's an issue -- for high assurance without regard, which has been the problem for prior compatibility or compatibility of prior systems or other bad choices that may have been made in the past?

MS. KRANINGER: I think the points that you raise are very important for us, as we move forward with this. I think that if the Secretary had had the opportunity to speak, he would have probably nailed this one out of the ballpark. But the two things he has

talked about most recently with me are really, you know, we obviously have to be conscious of those things. We've got to make the best choices with respect to the technology and have the technology, frankly, again getting back to my earlier point, support the business. You know, what is it that we actually need and want this to do? So let's make sure that there's a line. And at the same time, though, because this technology, as you know, evolves constantly. I mean, there have been so many improvements, even in the past three years that we've been talking about, well, six years really that we've been talking about a TWIC idea, there have been so many evolutions there, how do we decide or when do we decide, frankly, you know what, we're going to implement; we're not going to wait for that next generation and next generation because we'll never get it going. That is certainly one of the things that is motivating some of the decisions that we're making and that you're seeing come out of us now. You know, we've talked about TWIC, we've talked about Western Hemisphere Travel, we've talked about Registered Travel. We've talked about these things. At one point or another, again, with smart choices, we have to actually decide to launch, and how do we do that in the best way, making sure that it's scalable and flexible on the technology side so that we can build on it into the future. So I think those things are challenges to me, in particular, because I have a number of moving trains. These things are already well underway. How do we start at least directing them, you know, to a place that makes sense. On the one card, too, I just wanted to make a point on that. I think that's a goal and a vision. Though, in many senses, it comes back to the business. It might not make sense to have literally one card, but how do we make sure we use interoperable technology, how do we think more smartly about how these programs do or do not align, and move forward in that fashion? And so that's the kind of framework that we're trying to put over the decisions that are being made today so that we are moving on a smarter path for tomorrow.

CHAIRMAN BEALES: Sam Wright?

COMMITTEE MEMBER WRIGHT: For six weeks on the job, you seem to have a pretty good handle on the enormous task in front of you. As perhaps the travel industry rep on the Committee, I would offer a couple of comments. One, in your job as coordinator, in a lot of cases you're looking for cooperation from others. And while a number of industry groups are included in that realm of who you need to have cooperation from, when you get down to it, it's really the traveling public that you need to engender the most level of cooperation. And the traveling public, I think, in the past, and while it's improving, has looked at a number of the screening initiatives as increasing the hassle factor in traveling. My point here is that I think you should include in your scope of areas of responsibility a notion of a PR approach, as well, to facilitate cooperation. I think the best example of this is that with the occurrences in London on flights coming to the U.S. that there was an immediate concern about carry-on liquids, gels, and what have you. That message was communicated to the American public, and almost immediately

people understood that they just couldn't carry those things onto planes. There was never any concern, even the next day, about longer lines or anything else for screening. People had just been communicated to. The change had been communicated, the necessity for the change, and you had voluntary cooperation at extremely high levels. I think you need to keep that education, if you will, of the traveling public in mind as part of a coordination activity.

MS. KRANINGER: I couldn't agree with you more that it's an essential part of the Department's operations and the Department's success. I think that is a great example of something that worked and something we have to continue to build on. Obviously, and you know well and heard it from others that have spoken, this is a partnership. I didn't talk at length about the size of my office, but you can probably imagine that, while I'm really excited about the type of people that I'm getting and I've had great support across the organization, the point that you raise is very much a strategic communications public affairs issue. But at the same time, something that I've noted just with my history of the Department, too, is we have to make sure that all of those external affairs people really have a good understanding and grasp of what the program is trying to accomplish and where it's going and why the decisions have been made the way they've been made so that we can launch this in a way that, you know, is effective and communicating to the public and as clear a message as was had with regard to carrying on liquids.

CHAIRMAN BEALES: Ramon?

COMMITTEE MEMBER BARQUIN: First of all, Kathy, I truly applaud your revival on the scene as a member of our subcommittee on screening. We continuously asked about a number of the issues that obviously your office now will have to address, including definitions and issues related to inventory of screening systems, etcetera. The question I have has to do, come back to this issue of the architecture and the interconnectivity. At the heart of my question is the issue of the database or databases because so many of these screening systems that we've seen are showing a fairly significant duplication of a lot of the data that is, in turn, then, in some cases, transformed. But by and large, a lot of it really sits or could sit in more protected environments and within organizations that, by statute, would be much, much more acceptable, I believe, also to the public. So I wanted to ask are you going to tackle that specific problem? And how are you going to deal, also, with the agencies that are partners in the home security process, even though they're not part of DHS, which we've also seen are participating in the advantages that they see in some of these screening databases that you have?

MS. KRANINGER: One of the things that I would say is that obviously the Department is a conglomeration here of different agencies and different histories and different data sets and authorities, and there have been many efforts to try to begin to put that together under a framework that rationalizes where it is and start to identify, you

know, trusted repositories for entry and exit data into the country. If we can have that and say, for example, that CBP owns it and then figure out what the rules are governing access to that and why and, again, reasons for it, we will be able to accomplish all kinds of things at the same time. Again, it's better security, it's better privacy, it's better transparency in terms of what are all of these different databases and how do they interact and where should you be going to get that kind of information. So I think, in part, this is, again, a history, a legacy issue. I think it's more than history, it's a legacy issue. And we have tried to put some parameters around that and are thinking about that moving forward in terms of what investments we make. So I would say that's not entirely my issue, though it is something I'm concerned about and interested in. It's something that the DHS CIO, Scott Charbo, is very much thinking about as he looks at the enterprise architecture. It's something that we are going to try to start imposing some, I guess, framework around for helping some of these programs that had been, frankly, trying to figure out where is the data that we need, what kind of data do we need, what exists, and what doesn't? So I think that's something very much in the lane of going forward. I wouldn't say that the SEO is going to have a comprehensive look at that. Everything that we're doing is going to be really driven by delivery of certain programs but, again, in a smart way, so that we're looking at those kinds of issues and not making them worse, frankly, as we move forward. It's setting them in a better direction.

COMMITTEE MEMBER BARQUIN: If I could just follow-up, would you consider, if it made sense, both from the efficacy as well as from some of the privacy issues, for some of these databases to sit outside of Homeland Security, like for example at the FBI?

MS. KRANINGER: I think the answer is yes, again, depending on what their business needs and legal authorities are for having that information and owning that information. But I think it does get back to what are best practices around, you know, trusted repository of certain kinds of data, who should own it and be responsible for it.

CHAIRMAN BEALES: Neville?

COMMITTEE MEMBER PATTINSON: Thank you. You said you have a great deal of challenges ahead of you, starting from where you are with the proliferation of credentialing that have come in the past. To start to bring those together, I think, is a terrific challenge, and I certainly look forward to seeing you can make. In looking at the programs you're dealing with, TWIC and RT and Western Hemisphere and so on, they're all identification programs. Some of them are more travel related, some of them are more just identification. You talk about one card and building on that. It's more of one credential, I think, which is more important. But one credential is vetted in a consistent way, is screened, is applied to the policies of each different program required so that you have one TSA-based credential, essentially. And then that can then be manifested in whatever form needed for each of the programs and if it's one card or multiple cards,

whatever appropriate. I think there are a lot of constraints on the actual cards in the various applications for visibility and visual aspects, as well. So it's, to me, really about having one credential more than it is about having one card. But the credential is the piece that needs to be vetted consistently against those policies and then has attributes that show your authorization to access the various services. To be a TWIC holder, as well as a Registered Traveler or whatever, they have different roles that you'll need to project. So they may need to be in different forms, but, ultimately, one credential can be efficient in the verification. So I think it's important to have whatever the program is. The card can obviously authenticate the user, and then the card can then have the credential verified by the back-end systems. So the challenge is, I think, of all these different systems is to have the back-end being able to verify and authenticate the credentials to the individuals. So you have a great deal of challenges, and I look forward to seeing how you deal with those. And, certainly, I think the Committee is very dedicated to see how you manage the privacy, the redress processes, and so on, the adjudication process of all these systems, and certainly look forward to hearing from you again, I think.

MS. KRANINGER: Thank you.

COMMITTEE MEMBER SABO: Your comment about developing a framework for screening programs, in terms of the process to get there, I mean, you talked about, I mean, you eluded to the fact that there's a need for more expertise within maybe your organization but then the Department or the private sector, the complexity of all these initiatives that have already started, and now you're standing up your organization. When you look at the question like a framework for screening programs, have you thought about or have you thought through the process by which you're going to make that happen in terms of cross-departmental cooperation, as well as cooperation outside the Department? I mean, this body has developed some framework ideas about, you know, evaluating programs that may be useful, but in terms of specifically screening, how would you envision that process working? Would it be a cross-departmental body that would actually develop guidelines? The reason I get into that, as you know, trade-offs, you talked about supporting the business. But to get to Charles' comment about strong technology, strong security controls, sometimes the business slows down a bit if you enforce stronger security. Not always, but sometimes that's an implication. Cost might change. So brokering some of those risk trade-offs is an issue for program managers. They have the budget for the program, and, yet, you're trying to enforce some coordination. So I guess I'm looking to your philosophy or your practical views about how you will implement a framework both in developing it and then attempting to enforce it across these programs.

MS. KRANINGER: Let me talk about it exactly as you did on the developing and then enforcing because they are two separate things. First, on the developing end, there

have been a number of efforts over the past few years to kind of pull this world together and a lot of data calls around, you know, what are all of these programs, what are they actually doing and look like, including the HS PD 11 process that was terrorist screening, the Homeland Security Presidential Directive 11. And so what my office is doing is leading an effort that is across DHS. We've taken credentialing, again, as the first chunk, and I very much appreciate the points about identity management that are very much tied to how you would get at one identity or a person centric focus for the systems that DHS has and how we should manage that. But we are basically taking credentialing programs right now, taking all of those data calls that have been made, and looking at, frankly, these programs, looking at the life cycle of these programs and what they need to do. So, I have a chart I'm working on, so I didn't bring it to share with you, but it's basically talking about what does a program have to do across its life cycle from the policy decisions at each point in the way and certainly when it's started; the investment decisions, the privacy and IT infrastructure decisions that happen across the life cycle.

And then, if you take a program like TWIC, you have enrollment and identify proofing and vetting and card production and card use and verification and then the re-issuance, revocation, all of those things that feed back to start the loop, that's what we're doing. We're taking each credentialing program right now, looking at the data that we have about that program right now, and working with the program managers to at least get, okay, here's the picture of TWIC based on this framework. Not just TWIC, but then every other program. And then what we're going to do, and I frankly think vetting and identity proofing is the area where we can get a lot of, frankly, opportunity right off the bat is looking at how are each of these programs doing, in particular, their terror screening. What else are they vetting against? How can we make sure, both from an IT side, from a privacy side, from a security side, both at the system and, frankly, the end result, you know, are we getting the same answer? Getting into the weeds as to what are the name- matching criteria that are being used? What are the name-matching criteria that should be used? What is the state of the art that's out there to really do this in an effective way and start setting -- I'm shying away from the word "standard," not, frankly, because I'm afraid of imposing it but more because I want to make sure that it's not something that's too rigid. But a framework for how should you do vetting? And then, frankly, something for the next program that says this is how you do vetting and give us a reason why this doesn't work for you, but here's an office shelf capability that's ready to go. And then it gets to, again, our investment decisions. Is there a need for funding a new vetting engine that comes up from one of the agencies, or should they be using what the Department said is kind of how you do this kind of activity? So that's the view that we're taking. It's obviously going to take a long time to really drill into each of these issues, so we are looking for our best opportunities in trying to drill down into them. So that's the developing side. It really comes in to how do we chunk this, make it manageable moving

forward. The other side of this then is enforcing it, and my goal really is not to put in place another structure for review or submission but, again, leveraging what the Department already has. There is an enterprise architecture process and a joint requirements counsel and an investment review board, so all of those things are happening, development of a strategic plan. So it's tying into some of those process and enforcing them through those mechanisms and those existing reviews. And, of course, I have the ultimate, and that's the confidence of the Secretary and the Deputy Secretary, which has been tremendous in terms of trying to really drive these things home. So I expect to use all of those things to enforce it.

CHAIRMAN BEALES: Now, you may feel like you have a small office, but as a screening subcommittee, we have thought about, because we saw some real value in trying to do exactly what you're doing, and it was a daunting task. But I do think it's an important one and a potentially very useful one. I think we have time for one more question, and then we will take a break. Joe Alhadeff?

COMMITTEE MEMBER ALHADEFF: Thank you. I join the others in thanking you for the presentation. It's been very informative, and I think we all look forward to kind of the role the office plays, which we all thought was necessary, as well as the welcome of what seems to be the customer focus that includes customers that are outside the government, actually the traveling public and the visitors. It's not as if your staffing wasn't insufficient enough and your scope wasn't daunting enough, but I'm going to see if I can expand it in concept because, clearly, the framework deals with the other agencies that you're interacting with and, clearly, that framework is one that you would hope to enable across that framework, and you've talked very eloquently about interoperability. But one of the things you said early on was that you have visitors that are coming into the country, they go through CBP, and then you end up having them in TSA. They might bounce off other systems throughout the situation. Clearly, terrorism is not a problem that's unique to this country, so what's the international component of the coordination?

MS. KRANINGER: Completely appreciate that question because I think it's there. And I wasn't ducking the interagency question either because it's very much part of the discussion, too. But internationally there are a number of efforts within the Department to share biographic terrorist-related information, biometric information, and I think what we need in the government -- and it's not just the Department of Homeland Security, it's, frankly, with our partner agencies, DOJ and DOD and State most notably. But in how we prioritize what we're doing and how we operationalize it and how we share that, again, within the appropriate confines, whatever the agreement has been. So we need to do more work on that, frankly. There is a great priority on making sure that we have that information, and others have noted information that we're getting from Afghanistan and Iraq and how that is, who actually gets it, frankly, and then how they share it and how

CBP can use it to make sure that it's part of the admissibility decision process. You know, if we don't have the information, we can't use it and we can't keep somebody out of the country. So all of those things are related, and there are extensive discussions about that. I think probably the best example of what the Department has done is U.S. VISIT. I think it is tremendous, having been at the start of that program, and seeing what the, you know, initial concerns and push-back and what happened in Brazil right after U.S. Visit launched the fact that they were fingerprinting every individual who was coming into Brazil, and there was a lot of controversy surrounding that, to now we have countries the world that want to work on developing a similar system. And I think also, you know, biometrics, we have to be extremely careful about how we use that information. It is, you know, critically important to protect it, but it gets back to identity management and how do we actually identify an individual and, you know, protect the information about them and use that as, I guess, a trusted source of information about them. So I think on the international side, there are a lot of conversations. I think we have to prioritize what we're doing. My office will be involved in that. They're not involved to the extent that you're going to see my face oversees a lot. It's a bandwidth issue, but certainly one that I'm engaged in and watching.

CHAIRMAN BEALES: Well, I want to thank you very much for being with us today, and it's been most informative. I think you have a big challenge in front of you, as I'm sure you know. And I hope, at some point, we would be happy to be of assistance insofar as we can in what you're trying to do, and I think we have a lot of interest in an update at some point and just how things are going. So thank you very much.

MS. KRANINGER: Thank you.

CHAIRMAN BEALES: At this point, I think I will declare a break, in necessity, a break. And if we can resume at 10:30, we can come back for subcommittee reports and then the Deputy Secretary.

(Whereupon, the foregoing matter went off the record at 10:18 a.m. and went back on the record at 10:44 a.m.)

CHAIRMAN BEALES: If we could, please, come to order and continue with our agenda. We have arrived at the time that's scheduled for subcommittee reports, and when the Deputy Secretary arrives, whenever that is, then we will stop subcommittee reports and talk to the Deputy Secretary. And then we have more time for subcommittee reports this afternoon, to the extent that we need it. We have reorganized our subcommittees effective with this meeting. Under the old structure, we had overlapping membership in subcommittees, and so we had a number of people who were members of two subcommittees, and that made it very difficult for subcommittees to meet because most of those people found it hard to be in two places at once. So we've reorganized into three subcommittees that are non-overlapping membership in order to avoid that

problem. There is a Data Integrity and Information Protection Subcommittee that is continuing -- well, you'll hear what these subcommittees are up to in the subcommittee reports, so I don't want to say a lot about it at this point. But the Data Integrity and Information Protection is one subcommittee. A second subcommittee, which was the Framework Committee, is the Privacy Architecture Subcommittee. I should back up and say the Data Integrity and Information Protection Subcommittee that is going to be co-chaired by Ramon Barquin and Charles Palmer. For the Privacy Architecture Subcommittee that is co-chaired by Jim Harper and Joanne McNabb. And the third subcommittee is Data Acquisition and Use, and it will be co-chaired by David Hoffman and Richard Purcell. Under our process, when a subcommittee develops a report, it circulates to anybody in the Committee who is interested and expresses interest in that issue to review and comment on and be involved in. So people who have been involved in reports under the old subcommittees and retain an interest in participating in that project will clearly have the opportunity to do so. The process is built in a way that will let them do that. And if they've been working hard, we certainly expect them to keep working hard on those projects. So perhaps we could begin with the subcommittee reports with Data Acquisition and Use and Richard Purcell.

COMMITTEE MEMBER PURCELL: Thank you. Thank you, Howard. I'll keep this short. Our subcommittee has been working for some time and continues working on a report, a paper with the working title of "Public Agencies and Their Use of Commercial Data." As we reported in the past, focused on the implications and the policy framework that is consistent with our other committee's framework that approaches the acquisition and use and sharing of data that is gathered from the commercial world. We are hopeful that we will be able to report out that paper at our next upcoming meeting. Secondly, we are preparing the groundwork for our next foray, which will be directed toward emergency response and the policy implications of data and information management for first responders and public agents that are involved in emergency response, whether they're manmade, natural, or biological in nature. And it's a very complex area that we're just embarking on now, so those are our two major efforts at this moment.

CHAIRMAN BEALES: All right. Thank you very much. Data Integrity and Information Protection. Charles Palmer?

COMMITTEE MEMBER PALMER: Thank you, sir. Our work on the "Old Technologies and Best Practices" paper is continuing. We certainly appreciate the input we've received at the last meeting from those providing testimony, as well as the numerous individuals who button-holed us during the breaks. Sometimes, that's the most productive transfer of information, or at least more efficient. And we do appreciate that. And, of course, we also have received now a lot of input from the Privacy Office itself. It's sort of the way it proceeds as a committee releases something to the full committee, to the

Privacy Office, as well as the rest of the committee provides their input, and we appreciate that very much. We also continue to get input from various components of DHS. Again, we're sort of making ourselves known that we are studying this, and the other parts of the agency or the DHS that are busy trying to get things done are finding out about us and then running over to see if they can help us, as well as us help them move forward. So we want to make sure that these other components of DHS have the opportunity to work with us, as well as to ensure that our new CPO, Mr. Teufel, and members of the committee that have joined as of this meeting, will have the opportunity to contribute, as well. So our goal is to have the next draft available very soon to be shared with those members of the committee and privacy offices that are interested. And the ultimate goal is to have the paper submitted to the full committee officially for approval at the next meeting in December. Thank you.

CHAIRMAN BEALES: All right. Thank you very much. And Privacy Architecture, Joanne McNabb.

COMMITTEE MEMBER MCNABB: We're working on three continuing projects, one of them related to some recommendations on redress. We're happy to hear today from the Office of Screening Coordination and are looking forward to hearing from Jim Kennedy this afternoon. And we don't have a paper ready to go on that yet. We are also continuing some investigation on the procurement or acquisition process for technology with an eye to potentially suggesting an earlier insertion of privacy considerations. And I've already started talking to Peter Pietra and looking forward to hearing more from him on how that process is working at TSA. And, finally, we are embarked on a joint project with ISPAB, the Information Security –

COMMITTEE MEMBER SABO: Information Security Privacy Advisory Board.

COMMITTEE MEMBER MCNABB: Right. Thank you. I'll learn that yet. Which is a project involving the review of the Privacy Act and other federal regulations on privacy, in light of new other regulations for government, in light of new technologies and procedures, in an effort to identify whether there might be gaps in the regulatory scheme.

CHAIRMAN BEALES: All right. We didn't take a long enough break, did we? Or we didn't have long enough reports. Right. Can we take advantage of a couple of minutes? because we didn't have a chance to ask questions to Hugo this morning when he spoke because we started off behind schedule. And now that we're ahead of schedule, maybe we can go back to the beginning of the schedule and catch up. So are there questions from the Committee for Hugo? Lisa Sotto?

VICE CHAIR SOTTO: Thank you, Hugo, and we're just so delighted that you're with us. I wanted to ask you, this is not something that you commented on, but I thought it would be appropriate to talk a little bit about what you all have been doing as part of an

interagency group to study security breaches and best practices in information security. I know you've been involved in that effort, and I think I read very recently this week that some draft guidelines were just issued. If you could comment on that, I would appreciate it.

SPONSOR TEUFEL: Sure. I'm pausing here because it's been a busy last week or so, and I'm trying to remember. Which guidelines are you referring to?

VICE CHAIR SOTTO: On security breaches and best practices with the OMB.

SPONSOR TEUFEL: Okay.

VICE CHAIR SOTTO: They were not issued by OMB. It was –

SPONSOR TEUFEL: I think OMB was involved, and Toby actually has been working on this. I'm happy to have her come up.

MS. LEVIN: We didn't have this on the agenda, actually, to brief the subcommittee, but it's a great opportunity. I'm glad you asked. The Identity Theft Task Force, which was the White House Presidential Task Force that was convened with actually member from all the departments, secretary-level, and departments and agencies met on Tuesday, yesterday, the 19th, and reviewed recommendations and have accepted the interim recommendations with regard to identity theft, focusing on public sector steps. There are still a number of other recommendations that are under consideration. And the Identity Theft Task Force had a working group, and I was fortunate enough to participate in several of the sub-working groups on public sector and private sector. And the recommendations specifically that were issued address, first of all, having OMB work on providing guidance, on breach notification, and that means interagency efforts since OMB has interagency working group that has actually been working on that issue. So I suspect we'll see guidance for the federal government with regard to breach notification, as well as having OMB work with the agencies to review use of Social Security numbers with an emphasis on reducing the use of Social Security numbers in government programs. So that will be quite an auspicious undertaking. These are interim recommendations. These recommendations haven't been finalized. They will be approved for final implementation I think probably in November, at the next, at a later meeting. But I think they indicate that OMB and the federal agencies take very seriously the events of this past summer. You talk about lighting a fire under everyone's bottom, the incidence of this past summer with regard to federally-held data I think indicated that we all need to be doing a better job with being a steward of the information that we have. And so OMB was very quick to respond, agencies were very quick to respond, and it actually was joined with the Identity Theft Task Force effort. That effort had to come out with the Presidential Executive Order to set up the task force and had been underway for some time. So it actually, the timing of it worked out very well in terms of getting

mobilizing support and interest in the effort, and the very aggressive agenda and time frame to come out with specific results, which were just reported in the press this morning.

SPONSOR TEUFEL: Toby, we've been working very closely with CIO on this, have we not?

MS. LEVIN: Yes. In fact, Scott Charbo was one of the co-chairs of the interagency effort. This has really brought together, I think, privacy officers with the CIO officers within the various agencies to work closely to address these issues.

VICE CHAIR SOTTO: I think that sort of holistic approach is so critical, and I applaud you for doing it that way. Just an offer. I think a lot of us around this table have experience with security breaches over the last year and a half, so, to the extent that you need any assistance –

MS. LEVIN: I appreciate that.

VICE CHAIR SOTTO: -- I would offer any members of the Committee.

MS. LEVIN: Thank you.

SPONSOR TEUFEL: I'll mention, because it's an opportunity to comment on Toby and the fine work that she does. And Toby is fabulous. Toby is a superstar among superstars. Before I even got into the job, there was an incident that turned out to be not a significant incident that occurred two or three days before I formally and officially started in this position. And I was frantically that weekend reading up on this stuff, as well as working with Toby by Blackberry to deal with the situation where one of the components had inadvertently placed material, personally-identifiable information, on the intranet that was not easy to find. But if one were, by intent or happenstance, to come across it would find a tremendous amount of stuff about a tremendous number of people at this particular component. And so we worked very hard on that that first week that I was in the job working with the CIO's office and dealing with these issues. And, fortunately, it turned out to be not a significant issue, and Toby is in the process of completing her report, her review of the situation.

CHAIRMAN BEALES: John Sabo?

COMMITTEE MEMBER SABO: Just a question for Hugo. I mean, your commitment, I mean your bringing your commitment and background into what many people see as an incredible team and a very strong commitment by DHS to address this set of privacy issues, and I think proof of that is -- I think in your opening comments you talked about the use by OMB of your template. And I want to link this to our little Privacy Architecture Subcommittee. We're doing this joint project with the ISPAB, which is the NIST Committee, and the NIST Committee in 2003 issued a paper which talked

about the need, and it included information sharing as one of its points, the need for federal agencies and the expertise in federal agencies to begin working across agencies together to address privacy management issues and privacy policy issues that affect multiple agencies, exactly the kind of thing we're talking about. And DHS and you -- I'm getting to a question -- and you've actually shown that leadership, you've shown the leadership because you do periodicals, symposia, and workshops on privacy issues, and you're bringing private sector experts and the public, and you have those workshops. My question for you is, you know, now that you have the experience of working OMB and having some of the instruments and tools you've developed used by them, have you considered or will you consider organizing similar workshops across the federal government for federal government privacy practitioners? Because that will really fulfill one of the key recommendations of that NIST paper written in 2003 and really reaffirm your leadership and expertise across federal agencies and particularly for programs that cross departments. So it's a question. Will you or have you ever -- no.

SPONSOR TEUFEL: Yes. I think it's a fabulous idea. To relate to you something that I did in my prior positions in the administration, both at Interior and here at DHS, I put together a group called the General Law Working Group, which was managing general law attorneys at the various Executive Branch agencies and some of the independent agencies. And the reason that I did that was that I found we often address the same issues, but we didn't always communicate with each other, so there wasn't coordination, and we didn't learn from each other's mistakes and successes. And in the five years that I had the two, up until this one, the two best jobs in the federal government, I gained a tremendous amount of experience and benefit from working with my colleagues at the other Executive Branch agencies. I will tell you that we do some of that now. I was at a meeting yesterday with Dan Sutherland and Kathy Kraninger, some folks from State Department and some of the other agencies that were involved in the matter, and we were talking about privacy issues and how to address privacy concerns with this particular program that we were looking at. And in doing so, we were looking at the experiences of commerce and FTC to see how we would better accomplish that. Having said that, sure, that's an ad hoc approach, and there is value to, if not formalizing that through the use of workshops, bringing together our colleagues at the other agencies so that we get to know each other and we can work together because we are more effective if we do so.

CHAIRMAN BEALES: Joe Alhadeff?

COMMITTEE MEMBER ALHADEFF: Thank you. In your other conversation with us, you had talked about the utility of PIAs, the success of the template being adopted, the different times at which one may be run, including kind of the life cycle concept that as things change in a system you may need to run new PIAs related to it. Because a template

is comprehensive and, as we've seen in some of the PIAs that have been published, the answers are fairly substantial, and especially as organizations go through perhaps their first PIAs. So since I'm not sure that cloning technology is sufficient to get 10 or 15 Beckies in place, I was wondering, one, whether there's anything we can do, but, two, what your thoughts were on how to meet the burden of actually reviewing the PIAs that are there and how to kind of move that process forward, instill the desire to complete the PIAs in all the appropriate organizations and have them done in a way that allows the staff to be as efficient as possible.

SPONSOR TEUFEL: Well, it's funny you mention that because earlier this morning, during the presentations, Becky and I actually were exchanging notes. We've probably got 500 PIAs coming up, which is, roughly, two a day for me to sign. I was in Trier, Germany in 1984, and I was doing a summer study program abroad. And I had not appreciated the Air Force base was not far from Trier, and I remember taking a shower before I went off to school, and I heard some F-16s flying overhead, and it was disturbing until I realized that they were on training. But, of course, after September 11th, anyone who has been in this town, when you hear planes coming overhead in something other than a normal pattern, it tends to get one's attention. I was driving by the Pentagon on September 11th on my way in late and listening to the news reports and frantically trying to get a hold of Interior security officer because something obviously was afoot that morning. But I digress. We were talking about the 500 or so PIAs that we have coming up, which would be about two a day. And I read everything, and I often send things back because I want to make sure that we do it right. And it's not that Becky and her folks don't do it right. They're tremendously competent, very capable, and very hardworking, and very good at what they do, and, last but not least, very bright. But we want to make sure when these things go out, they go out properly. And so you think about 500 of these things, and it's not like I don't have other things to do. So in our conversations on how to do what we are charged with doing more effectively, looking at our statutory authorization, looking at what other legal authorities do we have and policy authorities, we're looking to see where can we be more efficient generally in the office. And then specific to PIAs, where can we be more efficient? I hate to use the word, but because words are failing me right now, is there a triage approach that we can, on the more routine PIAs, not be as detailed and put as much work and effort into. And that really doesn't capture the essence of what I'm trying to relate here because every PIA is important. But there are some that are going to be very significant, very high profile, very controversial. So the brief answer is I'm not sure what the answer is yet. The easy answer is always more bodies and more dollars. I don't think that's it. I would suggest to you that when we meet again in December, we take up this question again. And I will report back to you on what we have found, what we've come up with, what we're doing.

CHAIRMAN BEALES: That sounds great. Ramon?

SPONSOR TEUFEL: And I'm happy to be the opening act for the Deputy Secretary. I'll be here all week.

COMMITTEE MEMBER BARQUIN: I'm just going to ask you the same question I asked Nuala the very first time we met, which is one of the top two or three specific things that you would like to get help from from this committee.

SPONSOR TEUFEL: It's not specific but, generally, technology is within our statutory mandate, and that's something that we can always use assistance on. I think we're going to be looking at Real ID. There may be some questions there that we want to talk to you about. And, you know, frankly, I would say technology is probably the biggest of our concerns.

CHAIRMAN BEALES: Neville?

COMMITTEE MEMBER PATTINSON: Thank you. Hugo, I wonder if I can certainly ask if you have enough tools at your disposal with regard to influencing the various programs that go forth with the PIAs and so on? Do you feel you have enough stick? I know you're very collaborative in the way you work with the program –

SPONSOR TEUFEL: Yes.

COMMITTEE MEMBER PATTINSON: -- and building the privacy from the beginning and so on. But, ultimately, if the PIA comes out, which seem to be perhaps not the right conclusion or the right analysis, do you have enough empowerment to correct that or to advise them further? What is your, effectively, your veto capability?

SPONSOR TEUFEL: Well, as Mark and Kathy before me, I, too, believe in the unitary executive, and so I'm of the view that I don't need or this office doesn't need further authority or further power in order to accomplish its mission. I serve at the pleasure of the Secretary and the Deputy Secretary. They put me into this office. I have worked with them in the past and, in fact, now at two cabinet-level agencies have advised cabinet-level and sub-cabinet-level officials sometimes on very high-profile and sensitive and controversial matters. And I could not do and I would not have done my job properly had I not been able to advise them on those things and advise them candidly as to what the situation was. So I want to reiterate I don't believe this office needs further power in order to accomplish its mission. I wasn't here at the beginning of the department, but I got here right at the first anniversary of the effective date of the Homeland Security Act and a couple of months before the one-year anniversary of when it actually stood up. And it surprised me getting here how, and I used this line before, even bureaucrats will return to a state of nature and refuse to participate in any sort of well-ordered system in a new agency. So it was difficult in getting the 22, and sometimes people say 22 but I really think it's more like 30 or 35, pieces of different things from different agencies and getting them all to come together and work together. And certainly

it was the case for the Privacy Office. It was where I was over in OGC, and I think you'll ask anybody at the department level that there were difficulties in getting this thing fused together into one team for the one fight. We're three years, three and a half years old now, and there is some maturity, one. Two, we know each other, and by "we," I mean the folks who are decision makers and those who advise and counsel them. And Kathy is a great example, having been here and worked at Transportation and then for Secretary Ridge, going up to the Hill, and then coming back. So she has a lot of experience and knowledge and a lot of contacts within the department, as do I from my position advising and counseling senior management on issues relating to management and operation of the department. I've worked with and advised all of the folks that I had referenced earlier in my opening remarks. And I'm glad to see the Deputy Secretary is here, so we'll get back to that question. Sir, it's great to see you. Yes, indeed. I was just fielding some questions. No, sir, I was happy to be the opening act, and there were no rotten tomatoes, and so now you're here and so I will introduce you, sir, if you don't mind, and then we'll have some remarks from you.

On March 10th, 2005, Michael P. Jackson was confirmed by the U.S. Senate to serve as the Deputy Secretary of the Department of Homeland Security. In this role, he serves as the Department's chief operating officer with responsibility for managing day-to-day operations. Recently, he served as Senior Vice President at AECOM Technology Corporation and was responsible for government relations globally, as well as serving as the chief operating officer of their Government Services group. Prior to that, he was the Deputy Secretary at the Department of Transportation from May of 2001 to August 2003. And while that department's chief operating officer, he helped to stand up TSA, which is a remarkable, remarkable feat. Prior to that, actually in 2004, Mr. Jackson served on the President's Commission for Implementation of the United States Space Exploration Policy, and the Deputy Secretary also worked in two earlier previous administrations. In the Administration of George Herbert Walker Bush, he served at the White House as Special Assistant to the President for cabinet liaison and as Chief of Staff to the Secretary of Transportation. He also held several positions reporting to the Secretary of Education in the Administration of President Reagan. The Deputy Secretary graduated from the University of Houston with a BA and received a Ph.D. with distinction from the Government Department at Georgetown University in 1985. And, sir, I'm very glad that you're here.

THE HONORABLE MICHAEL JACKSON: Thank you. That just proves that I can't hold a job, so I am glad to have this one and I'm glad to be with you all. And thanks for having me, and thanks Hugo. I just want to say that I know that you all are trying to help Hugo adjust to his new position, and I want to thank you for that. He's got good experience and has a good ear and will be disciplined and engaged with you and supportive of your work, and he has our strong support. I'm here today subbing on behalf

of the Secretary, who came down with the flu and called in sick for the first time in 19 months for the morning at least. I don't know what will happen in the afternoon, but he's trying to get his voice back. He had lost it or was on his way of losing it last night, but he did call this morning and say he hoped that I would give his best regards. So consider them given. I think I met with this group when you were first started, and I've subsequently read several of the papers that you have done, including one that I had asked you to try to take a preliminary look at Secure Flight. But you also did a paper related to the use of private data which was associated with that issue. I've looked at your agenda of issues that you are setting for yourself to help us with, and I'm eager and grateful for what you've laid out ahead of you.

I think it's very helpful for us to have a conscious and a nudge and a set of advisors that we can turn to say, "Look at these things, guys. This is what's important, what's missing, where you made mistakes, where you ought to focus your energy, attention, and how to think about some of these issues." But the privacy issues for us are sort of like a working opportunity to stub our toe. And we just have to make sure that we are educating ourselves adequately and embedding into the DNA of the new department a sensitivity to privacy. We have constantly, I think, found ourselves in this sort of impulse to say that privacy issues provoke a balancing act conversation. And I think that's fair in a lot of the issues where we bump into Privacy Act concerns that we are facing a determined enemy. This determined enemy is trying to hide from us, trying to obscure, lie, and deceive, and penetrate various systems that we've set up to protect the security of the country, and it's more complex because of its international character in that we have to share data across boundaries, state boundaries, across organizational boundaries within the U.S. government, across global boundaries with other nations. So it poses for us a series of constant opportunities to stub our toe or to do something in a sort of ham-handed or incomplete way. So, again, I think that the work that you're doing with us is important for us to have this set of wise women and wise men who can help us just to make sure that we've got our compass oriented right.

The touchstones for us of trying to use the Privacy Act, even in cases where maybe it's not absolutely clear that you're legally obliged to do so, I think instills us a type of discipline with the system. The system itself of the privacy impact statements and the work that goes with it is a discipline, and sometimes it's a pain in the place you don't want to have a pain. But it is a way of trying to help us stay on track and avoid errors. It's also a way of helping the public feel comfortable that we're going to be responsible stewards of the work that we have to do. And that's a sales job, I think. You know, the concerns about the government use of private data and of data that we acquire in the course of the department's business is a real valid thing for people to probe us with and push on us with. I'll give you just one example. We have this whole WHTI initiative of using border-crossing cards, which are a proxy for a passport that they are, in effect, a flash pass, like

the NEXUS, SENTRI, and FAST cards that we're currently using. We're congressionally required to produce this new lower cost card. We have focused on using a biometric vicinity card. We know there's some issues about proximity versus vicinity that people are concerned about. And so what we're trying to do is, A, understand the technology in the right way; B, write the program rules and guidance and specs for the technology acquisition use and our notifications to the public about how we're going to manage all this in a way that will try to allay fears or address any concerns that people might have. I think that we're doing that in a disciplined and systematic way and, for example, by not putting data about the individual on the WHTI card but rather just having a number which ties back to a database which itself is behind a firewall is part of our concern about having a system of systems of layered protections for the privacy of individuals associated with the use of a card like this. So what I would tell you is the Department is spending a considerable amount of energy trying to think in the right way through these clusters of problems. I think that we will, you know, have to make sure that we find also ways to reach out to the public to listen carefully to what concerns might be in various different areas of the work that we do. And you all can be a little bit of a sherpa to tell us the ones that are more sensitive, where you see flashpoints, concerns, issues, and problems. So I know that, in looking at the agenda, you're sort of getting a little bit of DHS 101 update, and it may sound repetitive to some of you. But the point of hearing from the multiplicity of people at the Department is to try to make sure that you're in possession of a good understanding of where we're moving so that if you think that, as a group, there's some issues or opportunities to help us work in a certain area that you'll put your hand up and say, "Hey, I hear you're trying to do these types of things. Let's talk a little bit more about that." So I think I would propose to stop for a second and just maybe open it up for questions, conversation, and discussion with that brief sort of introduction. Anybody want to start?

VICE CHAIR SOTTO: I've been talking too much, so I would invite other committee members to join in. Thank you for joining us. We deeply appreciate it and know that your schedule did not permit this, but thank you for making time for us. You talked about the fact that privacy is an opportunity to stub your toe, and there's no question that that's true. I would reshape that a little bit and say that, in fact, it's an opportunity, and where it's an opportunity, I think in particular, is on the world's stage. We are viewed, rightly or wrongly, in the United States as not having adequate, the European world, privacy protections in place. And I think it's very important for us to re-frame how the rest of the world sees us, and DHS is a very, very good place to start because we have, within the Department, there's such a robust use of data, and there's so much sensitivity with respect to data that DHS collects.

THE HONORABLE MICHAEL JACKSON: I understand that, and I've spent recent time on several issues, like the PNR discussion with the EU where that's particularly true

and clear, and it comes back to this balancing act. In fact, leaving aside how we talk about this and how we communicate accurately our commitment to privacy protections, the facts start with a need to be able to gather and, in an appropriate way, use data that is helpful to us in finding terrorist patterns and, in particular, terrorist travel patterns. So then we get into a whole series of questions of how can we do that in a respectful way with enough transparency and with accountability in the process to make it work right. We do probably carry the burden of a lot of global mistrust of the U.S. government as a starting point, so we have to bend over even harder to lean in to making sure we communicate. I take the point as a very important one and a valid one, so agree.

SPONSOR TEUFEL: And you know, as you well know, Lisa, the American European models are not the only models, you know. The Asians and APEC and Vietnam recently. John Kropf from our office was working very diligently on those issues.

VICE CHAIR SOTTO: And I think he's viewed very favorably, as are the efforts of the Department and the APEC arena. Thank you.

THE HONORABLE MICHAEL JACKSON: Just real quick, that's a good example. I mean, we're talking about PNR data and advanced notification issues with the EU. But if you look to Australia, for example, I think they have some very useful tools in the way that they handle pre-arrival notifications and the like. And so there are just different business models out there, and we should keep our minds open to as many of them as we can.

CHAIRMAN BEALES: I was just going to ask what is the status of the negotiations about PNR data and what, if anything, can you tell us about that?

THE HONORABLE MICHAEL JACKSON: Stewart Baker went over there at the very beginning the first week in September. They've had video teleconferences between the EU staff and Stewart and our staff. This week, we've had interagency conversations within the multiple agencies who have an interest here, particularly Justice and State being important players in this role but also defense and transportation in others. So there's been a good administration-wide look from multiple different parties at how we're trying to work through that. And I guess the punch line is that we're trying to find a negotiated approach that is acceptable to both sides, and that's an honest and ongoing conversation. And we are mindful of the time that the European court put to try to resolve this, but I would say, also, that it was a somewhat arbitrary timetable, so we're not feeling that that's an everything-turns-into-dust on that date problem, honestly. But we are trying to keep a very fast pace. Conversations will be more this week, more next week, and we'll see where we go.

CHAIRMAN BEALES: I think Lance Hoffman had the next question.

COMMITTEE MEMBER HOFFMAN: Thank you. I appreciate your observation. I think it's correct about the Committee being a conscience and a nudge and a set of advisors all in one. How are you going to feed in these insights you get from all over the world, as well as internally, into the procurement process early enough so that they'll do any good, so that the train has not left the station by the time you get these insights and want to implement them?

THE HONORABLE MICHAEL JACKSON: Well, part of it is, I'm going to say that you all are helping to form an overall lay down of sensitivities and of issues, so on. You know, how we use commercial data, what type of privacy notifications we make, what are the redress provisions that we build into screening programs. I know Kathy Kraninger was here talking -- I don't know where you're hiding, Kathy. Oh, there you are. About her job, and we're trying, for example, in Kathy's world to bake into the policy integration around all these screening programs a continuous presence from the privacy shop and a sensitivity to those issues so that we can say in the design of the next generation of integration that we're asking them to be at the table. I'll give you an example. We had a fundamental decision to accelerate on a different timetable and a somewhat different business model but not, you know, wildly different, the implementation of the TWIC program. So at the beginning, we asked the Privacy Office to give us some counsel about how to do this TWIC program. And if I'm not mistaken, we had the Privacy Office sitting in on some of the core design conversations so that we would say, all right, so let's think up front how we're going to handle redress, for example, for people who feel like we've rendered the wrong judgment. How are we going to manage the privacy protection as we go from the intake at a seaport, which is essentially an outsourced enterprise, to moving that data across a DHS network into the background investigation switches that we have to check for things like the presence on the terrorist watch list and the like? How do we then flow the adjudication process of the redress work into a more robust departmental switch? Those sort of things. So I think part of how you fit in is to look at the whole with us, flag particular processes, core, attributes of successful programs. And then our commitment is to try to make sure that the Privacy Office is baked into this stuff as much as possible. And I said, when Mike Chertoff and I talked to Hugo about this job, I told Hugo very directly he has a, I think I used a somewhat less polite word, but a red flag that he can throw at the deputy any time he wants and say that this is something that you need to go work on or a problem that we see coming up and you have what I call bargaining-in rights, which is to come to the office, stand outside and knock on the door, and say, "Hey, I need you for three minutes to tell you about this, and it may mean that I need you for an hour to talk about something," but at least there's this access and interest. So he has access, I have interest. Hopefully, we can take your intelligence and use that funnel to help brand it together at the front end of these work streams as we design our processes.

CHAIRMAN BEALES: Larry Ponemon?

COMMITTEE MEMBER PONEMON: Thank you very much. This question may seem like a political football and, if it is, I apologize; it's not meant to be. Recent research shows that the Department of Homeland Security and TSA do not get great marks. In fact, they probably get very poor marks for the privacy trust of the American public. I'm familiar with that research because I've conducted it; my company has. So the question –

THE HONORABLE MICHAEL JACKSON: It doesn't sound political, but it certainly may be. I'm not sure.

COMMITTEE MEMBER PONEMON: I apologize in advance. But it leads to the million dollar question then: so how do you go about or is it important to improve the public's perception? If it is, how do you go about doing it?

THE HONORABLE MICHAEL JACKSON: Yes, Larry, it is really important, and that's why the research like that, in all seriousness, is important for us to look at. And I don't know how to do it, honestly. If I had a turnkey answer of how to do this, then we would be out making better progress. But, I think it's about communicating clearly and performing with disciplined and capable people in the field who act in a fashion that is predictable and disciplined and carefully managed in the sense of making sure that when we commit to do something we get it done and communicate what we're going to do and how we're going to do it.

I would think that if you did another round of questioning in the post August 10, the TSA stock went up a little bit because what happened here on August 10 was, overnight, TSA totally transformed the screening requirements for its organization. I will tell you they just performed terrifically, in my view. They were integrated with the industry when the British began the take-down of the cells in the UK. It was early evening. Prior to that point, there were five people in the Department that were read into what had been happening. Three days earlier, there had only been four people: the Deputy, the Secretary, and the two chief intelligence people in the Department. So we really went from four people knowing about this to executing the whole plan by virtue of the TSA administrator getting read in over the previous weekend, he and I working through existing templates of activity, how we would do things, still maintaining the operational security, but then executing their jobs. So I really think it's mostly about professionalism and performance and capability. If we do our job well and we don't stub our toe when we shouldn't, then I think the American public will see what I see, which is a tremendously committed group of men and women who are doing a good job, who need the tools to succeed, who don't have all of those tools at their hand at all times, and, you know, we'll get across that gap. Standing up DHS has really seen this across a whole group of things in the Department. We started out with a lot of tail wind and a lot of people thinking, oh, this is going to be easy and great. And then it got into the real hard

work of the Department, and about the time that that was hitting full stride of, you know, conflict and disagreement and really hard lifting, we had Katrina. And then it was easy for people to begin to characterize DHS as thimble bumpkins and failures and idiots. You know, we made a pile of mistakes and failed to have capabilities in place that we needed, but those capabilities had not existed for 30 years either. So we just have a lot to do in building this Department. I'm really confident that the next year or so we'll see a transformation in the way people think about this Department because we are gaining control of the border, we have eliminated catch and release as a program, we are doing good things to the secure world. You'll see some tweaks on that from Kip Hawley and his team here shortly on how we manage security against the particular threat of liquid explosive attack in balance with how to manage and move through the air space in a, you know, reasonably prudent way. So we are not going to just do things, stick with them, not be iterative. We'll try to be nimble, and I think you'll just see across a whole range of activities in the Department that we're going to be hitting a stride that the American people will feel good about. But, you know, they should expect for us to prove it, and we'll stick with it long enough to do so.

CHAIRMAN BEALES: Joe Alhadeff?

COMMITTEE MEMBER ALHADEFF: Thank you. And I guess this builds a little bit upon Larry's question, as well as some of the observations that have been made about a lot of the discussions we've had this morning about the concept of privacy being built in. Because if you're thinking about privacy, you have kind of two questions or two aspects that people deal with. One of them is the how, how to execute once you have a program in place. And I think DHS is getting some reasonably good marks on the how because I think there are processes that have been put in place, by the Privacy Office, like the PIAs and other things, that it really helped in some of the how. And while I think it's going on and I think it's going on more and more, as we've heard this morning, I don't think we get as much transparency, information, or comfort in the "whether." Do we really need this data element; is this the least intrusive way of doing this; some of the concepts that go in at the very beginning of thinking about a program before it ever gets into that. So I guess I'd like to hear if there's a way that considerations are being made to move those mechanisms and move that thought process further up even in the -- you know, it's one thing when you get to a policy, but in the actual concept of the program so that it really is more built in, and then what is the way to externalize that? Because, clearly, that's a process that has to be kept a little more in-house, but there still needs to be some transparency.

THE HONORABLE MICHAEL JACKSON: Good question on the whether and what you gather and how you do it and whether you need certain things. You know, at one level, it's easy. I start my morning off everyday at 7:00 with a CIA brief and an FBI

brief for our internal operational overnight briefing, internal intelligence people all together. And I tell you, it's a pretty grim picture sometime. I'll put it this way, sometimes it is not a grim picture. It is mostly a very sobering thing to start your day with. So it does sometimes, perhaps, create a mind set that says, you know, I'm going to swarm into this problem with everything I can think of. And I'm going to say that's the Coast Guard, I see one of my friends from the Coast Guard in the back there, that's really the Coast Guard Con-Ops. If there's a search and rescue call placed out, what you can know is every coastee within striking distance will run to that problem, right? And when we get the problem covered and the person saved or a clear set of assets on scene and able to do the job, they pull back. But there's a natural sort of first responders' impulse to surge every capability at a problem. So what you're asking is actually a very important, disciplined question, about how you bake into a job like DHS's a degree of self restraint, and so that's why I'm saying that there's probably no way to perfect that or predict that or manage that. It's a prudential judgment. It's what Aristotle says, that's the political virtue as prudence in making those balancing judgements. And sometimes I find myself pushing back a little bit and saying, no, you know, we can do with less but do with less a little better, faster, quicker, and more energetically. And that's the type of conversation we have.

So, you know, one of the things that we've tried to do is reach out to subject matter experts in a particular area to try to find that calibration point. So I'll give you just one example of a program I mentioned earlier, which is the TWIC program. We've reached out to a lot of the terminal operators, the labor unions, the ocean carriers, the captains of the port, the people who operate ports, and tried to say, "If we did this, what do you all think? How would this go?" And I just think it's a little, sometimes, tedious, but it's a really hugely important part of how we have to bake our operational work to yield that type of forcing us to think about what and how and whether all together in the right way.

CHAIRMAN BEALES: Neville Pattinson?

COMMITTEE MEMBER PATTINSON: Thank you, Mr. Chairman, and welcome Deputy Secretary and thank you for adjusting your schedule today, no doubt, to do the deputy work. You mentioned the Western Hemisphere Travel Initiative Pass Card, and this is the use of a static identifying number to identify a record within a database. You know, we have a subcommittee paper currently looking at RF-based technologies for use in identification and that. As we've disclosed earlier, it will be hopefully submitted at the December meeting of this committee. Obviously, we need to avoid privacy issues and lack of confidence in programs and, hence, we have a lot of people looking at this. And you indicated you have a lot of to understand the implications of moving forward with the program. Obviously, there are goals of the program that need to be met and, obviously, there are also privacy issues that need to be met. So it comes down to trust of the citizen

in the program. The State Department has gone through a great deal of public privacy issues over a few years, and they've learned a lot from that and understood how to perhaps involve security mechanisms to help protect the privacy of the citizens. So I wonder if you could expand on what would be the decision-making process from here onwards in order to bring the Western Hemisphere Travel Initiative Pass Cards to a resolution.

THE HONORABLE MICHAEL JACKSON: It's a process that's well underway, and you have to divide it into various different component parts. But, for example, just to start with the technology piece which you raise. We've done a fair bit of outreach to technology providers. For example, you mentioned the State Department, and we've had very close and, you know, continuous conversations with State Department on the RFID issues. They did have a lot of grief over the E-passport, and we've tried to understand why and figure out what lessons that might teach us in terms of how we manage this process, as well as the technology issues associated with it. I come from a world where, in the private sector, I was the COO of a company that ran New York EZ Pass, electronic toll collection systems across the country and around the world, and I have some personal history of the transponder issues and the RFID concerns. So it's something that I come to with enough knowledge to be dangerous, but a strong interest in it. So we're looking on the technological front at questions. For example, can we randomly scramble the number itself to provide another layer of protection and privacy into the process? So we've sort of concluded that that's a very promising technological extra element to add to the tool kit, but that it's probably not the exact first generation deployment that would be able to pull off. So we have a parallel track exploring that particular issue and making sure that if we can bring that online, can we do so with software modifications so as we don't have cards out there that are unable to accommodate that type of change. So I would say there's some technology questions that we just have to whack our way through, and we are doing so. Then on the program management side, we've had a lot of conversations with Canada. I have personally. I know Secretary Chertoff has had with his counterpart in Canada about their concerns about how we communicate, how we roll it out, how we get enough penetration into the market so that we don't create backlogs at the border, how we don't impose unfair burdens on groups of people that are trying. Like a large corporation, can we go in and actually help enroll on-site a large group of people in a different sort of way? The answer is we're open to all sorts of management implementation, program implementation, suggestions on ideas like that to try to say how can we make this work? We have got a congressional statute. It's not a "do this if you feel like it, when you get around to it", thing. It is you've got a law, you must comply with the law, and it has a date to implement it, and we're going to do that. And if Congress changes the law, then we'll look at the law and figure out what we're supposed to do next. But until such time as they do, we've got a plan and we will go through a spiral

development with it on both technology and program management and deployment and operations. But, you know, we're blowing forward. So if you all have ideas about that one, too, you know, welcome to the party, have fun, let's go after it.

CHAIRMAN BEALES: Ramon?

COMMITTEE MEMBER BARQUIN: You opened up your remarks by actually referring to some of the work products of the committee and talked about some of our thoughts of Secure Flight and commercial data. The question is, first of all, we're encouraged and certainly flattered that the Office of the Secretary has gotten some attention. But feedback force. Were they too high level, too much of the weeds, just right, so that, as we move ahead, we can try to target our focus here?

THE HONORABLE MICHAEL JACKSON: I'll give you -- what I would say is they were all great. And after I throw that one at you, let me say that they were different. And so the paper that I read and, you know, I can't be certain that I've read everything that you've written, but I did try to read the stuff that you're generating. The paper that I read on Secure Flight, which we talked about initially, as an area where we, as a department, needed and wanted your counsel and your work, that was a high-altitude, get oriented, how you think about this cluster of problems. And then you laid out a series of work products, like the paper on use of private sector data, that was more detailed. And then you have a couple, I think, in extreme that are, in essence, complimentary and supportive of that initial architecture and the Secure Flight paper, and you've got a subcommittee structure that's, I think, dividing the labor to work on those. So the one that I read on the use of private data I thought was good in that it gave the Department an architecture of how to think about it. You said here are questions you should ask, here are categories of issues that you need to use to get your brain around what these problems are, here's some facts that we've found, here's what, you had an interview with Justin Oberman, which either, dependent upon your perspective, raised concerns or solidified a course of questioning for us to take on. So I think all that was good. I think it's helpful. It's a delicate balance to be a nudge without being a pest. And I guess what I would say is, you know, when in doubt, go ahead and feel like you can be a pest. It's okay. I mean, you know, if our guys don't have a thick skin, they should go find another job because they'll be in constant turmoil and be eating antacids all the time. So it's okay to do it. I appreciate it in a respectful way that doesn't have the, "You idiot, how could you have done that?" tenor, and none of your papers do. So I was grateful for that and I was respectful of that, and I thought you were, in turn, respectful of the complexity of issues and the difficulty of having to steel through a pretty complex web. And so that's why I said I thought that they were helpful. And I, frankly, Hugo, think that probably, I don't know whether they're getting as much circulation in the management team as we should, but we --

SPONSOR TEUFEL: They will, sir, if they're not.

THE HONORABLE MICHAEL JACKSON: Okay. So it's a good thing.

COMMITTEE MEMBER PURCELL: A quick follow up to that. Are they timely? One of my concerns is it's a big committee, we have a lot of people. The processes, because our internal processes and factor rules make it difficult to produce the documentation that we are producing in a manner that's as timely as some of us would like. Is that a concern of the Department, as well?

THE HONORABLE MICHAEL JACKSON: Yes, it is. You know, the more timely, the more targeted you can be, the better. And I think that's why, you know -- Hugo's a lawyer so we'll have to let him bang me if I go wrong. In a FACA committee, you're constantly doing another one of these balancing games. It's right and appropriate and helpful that your deliberations have public nature to them, so that people can say, "Hey, you guys ought to think about this," or, "How could you come up with such a goofy idea as that?" And so that part is good. But it's also sometimes possible in a FACA environment to have a subcommittee, the purpose of which is not to provide consensus but just to provide input. So, for example, if we reach a point where we're working on a technical issue, like the WHTI card, and a couple of you have real subject matter expertise in that area and would be willing to talk to us if we had the, you know, the smarts to ask you, we can do that. And I think I would encourage Hugo to use the committee like that. Instead of trying to write a paper about everything, we can have, sometimes, a one-hour telephone conference call and say, "Hey, here's five ideas we're kicking around. What do you think of these, and should there be a sixth one that we missed?" So I'm going to say that I would encourage the Privacy Office to engage you in that way, as well, which is complimentary and supplementary to what you're doing and more, perhaps, timely in some cases, so that you're not reading about it after it happened but, rather, taking this line of question that we already talked about, you know, get in up front with some orienting counsel.

CHAIRMAN BEALES: We did that, to some extent, actually, with Secure Flight.

THE HONORABLE MICHAEL JACKSON: Yes, you did.

CHAIRMAN BEALES: And it was useful. We felt like we were being helpful.

THE HONORABLE MICHAEL JACKSON: No, and I heard back from our program manager about that and about your conversations with him at the time. I think they had a separate meeting on that topic with him, at least one quite protracted meeting, and I got a guy back in my office telling me what you said. So that was helpful.

CHAIRMAN BEALES: All right. We want to thank you very much for taking the time out of your schedule to be with us. We really appreciate it. We are glad to know that we're, hopefully, helpful, and we'll try to deliver you more light reading.

THE HONORABLE MICHAEL JACKSON: Good. Okay, thanks. I appreciate it.

CHAIRMAN BEALES: I would remind the audience that there is an opportunity to address the committee at the end of the day, at 4:30. If you are interested, please sign up at the table over here and get on our agenda, and we would be delighted to hear from you. At this point, we are going to take a break for lunch, where we are going to do various administrative tasks. So that part of our meeting will be closed to the public. We will resume again at the afternoon session that is open to the public at 2:00, and we look forward to seeing you all back here then. Thank you.

EXECUTIVE DIRECTOR RICHARDS: If you're planning to come back in, please be at the visitor's center no later than 1:45 so we can back and forth. And we'll have TSA and DHS staff at the door because we have to be with you at all times.

(Whereupon, the foregoing matter went off the record at 11:54 a.m. and went back on the record at 2:09 p.m.)