



Homeland Security

DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
FULL COMMITTEE MEETING
WEDNESDAY, December 6, 2006
Eden Roc Hotel
Mona Lisa Ballroom 1
4525 Collins Avenue
Miami Beach, FL 33140

MORNING SESSION

MS. RICHARDS: Good morning, my name is Becky Richards and I am the executive director of the Data Privacy and Integrity Advisory Committee and this committee is now in session. We will begin with Admiral Nimmich.

CHAIRMAN BEALES: Thank you, Becky, and welcome everyone to this meeting of Data Privacy and Integrity Advisory Committee.

There are a couple of housekeeping items before we get started. First, please turn off your cell phones. You can show us your ring tones at lunch. Second, as is our custom we have a public comment period at the end of the meeting and all we ask is you sign up at the back of the room with Lane Raffray and we will hear from anybody who wants to speak to us at the end of our public meeting.

Our first speaker today will be Admiral Joseph Nimmich who is the deputy chief of staff at the U.S. Coast Guard. He assumed that position in July 2003.

Prior to this assignment he served as commander of the Coast Guard Group Key West which provides high quality responsive service that contributes to all of the Coast Guard's strategic goals. Admiral Nimmich has enjoyed a very balanced 27-year career dividing his service between operational assignments both ashore and afloat. Admiral Nimmich has also served aboard the Coast Guard cutters Woodrush and Mesquite and has commanded the cutters Point Estero, the Red Beach and the Soral. He has held various staff assignments in both districts and headquarters including office of operational law enforcement, Office of Budget and Planning Policy. Welcome Admiral Nimmich, and thank you again for the wonderful tour yesterday.

ADMIRAL NIMMICH: Thank you, Mr. Chairman and you members of the committee for the time this morning as well as the extensive time yesterday afternoon to allow me to discuss with you one of the security gaps that we feel that we need to address in the Coast Guard.

I would like to give you a quick overview and restate some of the discussions that I had individually with some of you yesterday, then offer you a few minutes to ask me any questions and indicate my desire to work with you on any privacy implications that may come from our attempts to close this gap.

We looked very closely yesterday at vulnerabilities of our maritime infrastructure particularly in ports. With the uniqueness of the maritime environment that had grown over two centuries that allowed recreational boats to move right along side industrial facilities, and critical facilities, right along side of import/export and container terminals.

This being in an integrated environment that really developed over time without any rhyme or reason that creates a large vulnerability for us in creating a more secure environment.

Adding on to that, once the vessels move from their burning facilities there really is no vulnerability reduction capability other than an escort boat, and as we discussed yesterday there is very little decision-making capability for that Coast Guard coxswain to determine whether that boat that's coming at a cruise ship at a high rate of speed is a teenager who is joy riding or a terrorist who intends to take any type of negative action against that cruise ship.

Our ability to break that chain that creates the ability for a terrorist or somebody to take action really exists to the far left where there is more information and the ability to break the cycle when people are planning and doing observations and doing other things rather than that last minute decision for that protection.

There are no barriers, so you can move around the ships as they move, so we really do have to move further out. At the same time, if you recall, we talked about the fact that of all of the different modes of transportation the recreational boat is the least governed.

If I asked how many of you currently own cars, I would probably get 100 percent recognition that you all own a motor vehicle of some type. If I asked how many of you had driver's licenses in your pockets, I would get the universal response that everybody has a driver's license ... but we will not ask if they're valid or not. However, at some point in time in the past you proved your proficiency in both understanding the rules that govern how we drive cars as well as demonstrating your capability of controlling that vehicle. If you're a pilot and have a pilot's license that's an extraordinary level above driving a car as flying is much more difficult than is driving because if something were to happen in the air, the aircraft could then fall to the ground.

Whereas, if something goes wrong with a car you can pull over the side of the road. Likewise, maritime is equally as complex as is aviation where you are in an environment where the road moves while you move where it could be heavily impacted by wind as well as your ability to not see what is beneath you.

There can be potholes in the road, usually you can identify it so you can maneuver the car, but in a maritime environment with recreational boats you are required no licensing.

Well, let me recast that. There are five states that require minimal licenses and usually that's a written test only for understanding the safety implications. There is no practical exam that indicates that you know how to control the vehicle that you're currently owning and driving. None of those systems are interoperable and there is no interoperable registration system.

If you're stopped outside this hotel and you're driving a rental vehicle within a matter of minutes a State Trooper or that police officer can identify from license whether you have in fact had the ability to drive that car and if there are any warrants that are out for you as well developing information from the rental company.

If you're in our own car it doesn't matter if it is Washington State or Michigan they can determine whether the car is properly registered and whether it is owned by you, and if not, then who owns it and whether they have any information that the car may be stolen or relay retrieve other pertinent information to the police officer and none of that exists today.

What happens in the State of Florida routinely in the winter time as vessels are towed down from Michigan, Maine, and other states and there is virtually no way for a Coast Guard petty officer as we saw yesterday, doing the boarding on a vessel or a Florida Marine Patrol, to be able to determine if that boat is properly registered and if you're the appropriate owner all of which creates huge vulnerabilities.

It's a reality. There was the Cole attack in Yemen. The Lindbergh attack off Somalia, an attack on 3,200 in the Philippines all indicate that it is a low end easy technology for those who wish to do us harm to be able to use.

Will it be used in the United States? All I can tell you is that the first major car bomb attack in the U.S. was in 1983 at the Marine barracks in Lebanon. Cobart Towers in Saudi Arabia, the American Embassies in Africa, all were done -- well, the first two were done prior to the first bombing of the World Trade towers in 1993 and then we saw the results further on using vehicle borne explosive devices.

Is it possible? Absolutely. Are the consequences large? Absolutely. It is just not someone who is on a cruise ship and is an easy target. It tends towards what terrorists want to do. Attack what they believe is the decadence of the American public, but I will

tell you that there are chemicals that are moving on our rivers and on our waterways each and everyday that have implications far exceeding anything that a cruise ship could have.

There are chlorine barges, ammonium nitrate, the car bombing of the Oklahoma Federal Building was ammonium nitrate. The quantity that was used there is 100 fold than most of the barges that move around this country.

The vulnerabilities are there and the capability is there; we are really doing nothing on our information systems to be able to make some of the decisions that intercept those before we get to that 11th hour when a young coxswain is deciding to shoot or not shoot in a matter of 10 to 15 seconds.

So why am I here today? Mostly to make you aware of what we are trying to do with ports and to get your insights to the privacy implications, to look at creating a privacy impact assessment for you for the legislation that we're looking for.

We are taking small steps to begin with and we are looking for that same type of motor vehicle registration and licensing capability that exists today for your car, for your boat on the water.

I can tell you that there is somewhere between 13 million and 17 million recreational that are boats out which is a very wide span to have between 13 million and 17 million and one would think that I should be able to tell you a much closer number, but I really can't because we don't have an accurate registration system.

We need to be able to look at that. This has implications that go far beyond just the security we have talked about. I can regale you with case after case to choose one that talks about safety.

A young six-year-old boy just this past Memorial Day was down in Key West who was run over by a 17-foot boat with a 125 horsepower outboard on it.

The boy was snorkeling with his father who was about four feet from his father when he was run over. They had the dive flag up and their boat was in the general vicinity. He was doing everything right. The person running that boat was a 13 year old boy who is now in a detention center in Florida and he may be there until his 21st birthday depending how he reacts to his time in the detention center.

So two families that are destroyed because a 13-year old boy was operating a boat who really had no business being there who had not been trained.

He took a safety exam, but he did never prove that he could actually operate the boat. With that I would like to answer any questions you have and then I will solicit through Hugo and the privacy committee group's staff at DHS to go through a privacy

assessment to ask for your input so that as we move forward with the potential legislation we may address any issues you may have up front.

CHAIRMAN BEALES: Thank you, very much, Admiral Nimmich. If members of the committee have questions if you would follow our custom of turning up your tent and I would be happy to call on you. So we will start with John Sabo.

COMMITTEE MEMBER SABO: Thank you. Quick question. Have you thought through any of the data elements that you feel that you would be collecting as part of this system? My second related question is, am I correct that you would see the States doing the data collection and then passing this electronically through network to the Coast Guard database?

ADMIRAL NIMMICH: The motor vehicle model is certainly the one that we are patterning in on which would be state run.

Federal standards that the states would have to ensure that they capture, but then some sort of a repository. The motor vehicle database now is actually a not-for-profit group that has done the translation of all of the different state databases for cars into a system that the police officers can call into and get whatever information they need in a timely manner.

We look to model that. One of the things that we're working now with the states -- Well, it turned out that it actually paid for itself with the fact that there were many motor vehicles that were not properly registered and if they were two or three states away there was no really easy way to communicate that to the state that had the registration so they were losing the registration money and they found that out by working through the not-for-profit.

We are doing a study now that we believe will indicate that it is even worse for recreational boats that the states can self fund their registration systems and that it wouldn't be an unfunded mandate, if you will.

CHAIRMAN BEALES: Richard Purcell.

COMMITTEE MEMBER PURCELL: Admiral, could you explain to the committee and for the record the difference between your vessel inquiries into people who are in a vessel and the difference between that and law enforcement's access to people who are stopped in their motor vehicles.

ADMIRAL NIMMICH: Absolutely. As you saw yesterday in some of the briefings in order to be able to get any information there are about 10 to 15 different databases that manually have to be entered.

When a police officer stops a vehicle they make one phone call or one text message back to their station and they make one inquiry into the non-for profit which gives them

all the information as to any wants and warrants on the driver as well as any information that may be applicable on the registration of the vehicle.

We cannot do that on a recreational boat today and this could take as much as eight to ten hours to find the right people to give you information on registration when you go back to the states.

We just don't have the time to stay around for ten hours and we cannot inconvenience the boater to stay that long either.

Often we find out information after the fact and then you attempt to retrace them down particularly when there is a warrant that is out on the individual.

There is no requirement right now that identification be carried on a recreational boat. We often stop boats and have to take people's words for who they are because they do not even carry a picture license as required by a driver's license.

It would be very easy to just add on to the driver's license recreational boating validation that you can use just as you use with your driver's license now.

This would not be a new license that has to be given out but is just an added note on the driver's license indicating that they have passed the recreational boating operational requirements.

COMMITTEE MEMBER PURCELL: A quick follow up. Could you explain the probable cause basis for investigating a vessel that is at sea versus a driver who is on the road?

ADMIRAL NIMMICH: Probably at sea is the only environment now where you don't need to have any probable cause or a violation in order to go on board to inspect a vessel.

It has been maintained through the court systems for the last 200 years because of the mobile environment, the ability to move almost anywhere with the ability to evade very easily. There are no roads. You cannot put roads blocks up and it goes on and on.

The courts have maintained our authority under 14 USC 89 to do random boardings to ensure courtesy safety inspections and as a result of that if any other violations of laws are detected you can take action on those.

COMMITTEE MEMBER PURCELL: Finally, do you see any change on that basis to be altered by this proposed legislation?

ADMIRAL NIMMICH: No, I do not.

CHAIRMAN BEALES: Admiral, is there any evidence from the state licensing requirements that are out there about the impact of licensing or training on the safety

issues? Obviously it would be very hard to measure the impact on terrorism issues, but the safety issues are presumably much more observable and measurable.

ADMIRAL NIMMICH: We find that those people who have taken the time to take a safe boating course with the Coast Guard Auxiliary or with the U.S. Power Squadron have a lower impact of potential accidents than those who do not.

CHAIRMAN BEALES: Joe Alhadeff.

COMMITTEE MEMEBER ALHADEFF: Thank you. The Coast Guard is engaged in any number of activities many of which the public may not even be aware of, from a safety inspection to helping improve boating safety, to illegal immigration, to interdicting drug smuggling, to general patrolling of the waterways and all of these other things, and as you pointed out there being the example of the potentially drunk 17 year old who may be buzzing about versus somebody who is intending to do harm with the boat.

In the various stops in all of these examples, clearly there is an opportunity and a necessity to collect some information on some of these people which may run the gamut from a fairly innocent inadvertent action or an oversight of security to a more willful misconduct to actual criminal and potentially terrorist activity. Is there a way that you differentiate that information in the systems in how you maintain the information and the period for which you maintain it?

ADMIRAL NIMMICH: I cannot answer all of that. As to the period, I am not certain as to how long we maintain the information for that, but we do collect the information from all of those boardings that we do in our maritime law enforcement and information system. That is the standard form that captures the operator information as well as the owner information that is available at the time and why we stopped the boat and what it was we found on the boat. Those are maintained for a fairly lengthy period of time because as we move forward the next time a boat is potentially going to be boarded the first thing the coxswain will do is to go back and see when it was last boarded and what was found.

Frequently we will not board a boat if we found that it was just boarded. For a long time back in the early 1990s we were criticized heavily because as you move from one district to another district for, say, taking your boat from Maine to Florida as you moved through each district they didn't have knowledge that you were boarded prior and you may stop them four or five times with the same type of boarding with no violations found which becomes very frustrating to the boater.

What we have is a nationwide system where we can find out, why was it boarded last time and what was found?

Now, if in fact there was a violation that was found the last some time then we may board it just to confirm that they repaired the violation. I don't know the length of time. It

is law enforcement sensitive and so access is restricted to Coast Guard personnel and other law enforcement agencies.

CHAIRMAN BEALES: Ramon Barquin.

COMMITTEE MEMBER BARQUIN: My question is somewhat related. What we have found is that very often if the specific purpose where you are developing a system and are collecting data, I was thinking as you were speaking about the registration, if that purpose is not clearly defined and you stay within what you have fenced, then that scope pretty much gives rise to potential for misuse being the driver's license case in point where originally it was created to make sure that the individual in effect had passed the test and they knew how to operate the car.

Today it has become for all practical purposes a national ID and is not something that was intended, so my question is this: as you move ahead, what really is the purpose? Is it specifically tied to safety of recreational vehicles and how are you then going to deal with other legitimate needs where we have preventive terrorism and drug surveillance front, so what is your thinking in this direction?

ADMIRAL NIMMICH: We have sought some of these requirements licensing and registration long before 9/11 as a safety factor. We believe that we can reduce the number of injuries and accidents just by training people and ensuring that they know how to operate their vessel. Since 9/11 it has become far more critical because of the vulnerabilities that have been identified.

There would be the same as with your driver's license, there is the ability to utilize the information that you have provided through the licensing in order to ensure that we can run your name against terrorist watch lists and all of the other things that a driver's license does. We look to that as having the same capabilities that the driver's license does and that is where you get into the security aspect of it, but that same information that you're providing to get your driver's license is all what we are really looking for at this point in time.

CHAIRMAN BEALES: Ana Anton.

COMMITTEE MEMBER ANTON: I believe you mentioned that for recreational vehicles there is no need to have any identification with you on board. Does the same hold true for commercial vessels?

ADMIRAL NIMMICH: No, not at all. With commercial vessels their crews have well researched documentation with picture identification and we are working now to try to make that common with the TWIC process and as TWIC comes into play because merchant mariner licensing already existed, there are some implications to make sure that we don't double charge them for the same information that we are working off of, but all commercial vessels and crew members have to have identification with

credentialing where you have the capability of filling the position they are in, that they are First Mate or a captain and they have the appropriate licensing.

CHAIRMAN BEALES: John Sabo.

COMMITTEE MEMBER SABO: One follow up question. Are you envisioning on the DHS side, the Coast Guard side, since you are part of the Department, basically using any existing systems for the back-end of a database or existing networks for the transmission versus the building of a whole new system?

ADMIRAL NIMMICH: No, we would look to try to model the motor vehicle side which is not to have the states build any new system but to implement it on their existing systems and then use the non-for-profit center to be able to access that information.

We are looking to have this as a decentralized application on a federally run process with a federal standard set and then the states can implement that, but we are looking to work with the states to indicate what the potential cost would be and then potentially look through grants and other systems to be able to provide some resources for them to be able to set up their systems.

There are five states that now currently use paper testing or some sort of testing for the safety side, but there is no state that actually has a proficiency exam as you have with your motor vehicle.

CHAIRMAN BEALES: Do you use commercial data sources about boat ownership, and if so, how complete are those sources?

ADMIRAL NIMMICH: They are fairly incomplete and insurance companies are the only ones that really have any sort of data source that we can use and we do access those through the mutual agreement with them if there is an implication and usually that is a stolen boat or some direction along there where they have a vested interest.

CHAIRMAN BEALES: So that access is limited to those particular circumstances?

ADMIRAL NIMMICH: That is correct. We do not have routine access. We have to go through their systems and request access for a specific purpose. We do not have just general access to their databases.

CHAIRMAN BEALES: Mary DeRosa.

COMMITTEE MEMBER DEROSA: You mentioned the problem that you have with the variety of sources of information that are not compatible requiring separate searches and I am trying to get a sense of how this licensing issue is related to that. Do you see that as in some way a solution to that problem and if not what steps would you need to take on the database issue?

ADMIRAL NIMMICH: All of those other databases are incomplete. They are just databases, depending on what the state collects or doesn't collect, the first is minimal standard of what we need to see from the states and then utilizing the state system, so those systems would become more robust and should be integrated as I have indicated through motor vehicles where technology exists that would integrate the databases as long as there is a standard when collecting similar information so it can be shared.

CHAIRMAN BEALES: Admiral, putting aside the safety argument, as I understand it, the safety argument provides for licensing which has a lot of merit, but just sort of focusing on the law enforcement aspect of licensing and registration, it seems likely that the people we were most concerned about are not very likely to comply with licensing and registration requirements, that the burdens of compliance end up falling on people, where from the Homeland Security perspective there is not really an interest in registration information, although there may be for other reasons for safety reasons in particular.

I am just wondering what your reaction to that is. What is the value of a system where the bad guys are the ones who are the least likely to comply?

ADMIRAL NIMMICH: Once you have a system in place where compliance is required the anomalies are easier to find, as Tara said, when you go rent a boat rather than buying one, if you don't have the licensing then you can't get to rent the boat to begin with.

So that you are making it more and more difficult for them to use this venue to carry out an attack.

Additionally, right now it is pretty well known that probably one of the few places in the world where you can become anonymous is in recreational boating.

People who live throughout the keys who are on their boats that probably never had nor do they ever intend to have a Social Security number and they work through paper systems and cash processes so you don't know who they are or what they are.

Maybe we cannot afford that type of anonymity anymore. We do believe that not only would it help us with detecting those anomalies for potential terrorist attack but law enforcement in total.

I cannot tell you how many wants and warrants we executed for the Sheriffs' Departments in the State of Florida for people who are on fishing vessels or on recreational boats where this is where they found their refuge to escape law enforcement.

CHAIRMAN BEALES: Admiral, thank you very much for your appearance here today and we look forward to working with you to assist us as we move forward.

ADMIRAL NIMMICH: I appreciate it, and as I indicated, it is our intent to work closely with you to address any potential privacy issues up front so that as we move forward with legislation in the future that those questions are already answered before we get to Congress.

This is an area that they tend not to want to legislate in, so the more what we do for them and make sure they understand it, the better off we are, so we will be preparing a privacy impact assessment and we will look for your feedback.

CHAIRMAN BEALES: We appreciate that and we look forward working with you. Certainly we all agree that the time we need to think about privacy issues is up front and not after you have done it.

Thank you again for your time and your appearance today.

ADMIRAL NIMMICH: Thank you for your time and good day.

CHAIRMAN BEALES: Next on our agenda is a report from Hugo Teufel, III, chief privacy officer of the Department of Homeland Security.

He was appointed by Secretary Chertoff on July 23, 2006. He serves as the Department's Chief Privacy Officer and the Chief Freedom of Information Officer. Prior to joining the Privacy Office Mr. Teufel served as the first associate general counsel for general law at DHS. Prior to that he served as the assistant solicitor for general law at the Department of the Interior.

Mr. Teufel, thank you for joining us.

MR. TEUFEL: Thank you very much. It is great to be here in Miami. This is my second time that I have been before the committee. I have had a little time on the job which is helpful. I have a lot to tell you. I can probably answer more questions. I cannot guarantee that I will have an answer for every question that you all may have at the conclusion of my remarks.

Good morning. It is great to be here. I want to thank Admiral Nimmich who has, I believe left, for coming to speak to us. When I think about homeland security and homeland defense, the Coast Guard is at the top of my list.

You will recall not too many years ago, sixty or so in fact, the last time there were American and foreign born individuals who intended to do harm to this country it was a Coasty who found evidence of their activities on a shore in the Eastern United States during World War II. They are critical to the homeland security and the homeland defense mission.

Next, I would like to acknowledge those on the committee who will be leaving us. I want to thank you all, those who are staying and those who are leaving your service,

and I want to acknowledge the five who will be leaving the committee and thank them personally. First, Sam Wright who is not here. Thank you for your insight into the travel industry and your consideration of travelers. Tara Lemmey, who is here, thank you for your expertise in applying technology to help fight terrorism. Third, Joe Leo, who is also here, thank you for your knowledge and experience as a Federal CIO. Fourth, Jack Marsh who is not here, I want to thank him for his participation. Fifth, Michael Turner, I would like to thank him for his initial work on sharing in emergency situations. As always I would like to thank the committee for its continuing work in assisting my office and in advising the secretary and me on tissues of concern to you.

What have we been doing since the last time we saw you? As I indicated the last time we spoke I was in the process of looking at what we in the office were doing and how we were structured.

We have since bifurcated the office into a FOIA side and a privacy side to give greater exposure and prominence to FOIA. As you know in federal privacy law there are the three pillars, the E-Government Act, the Freedom and Information Act and the Privacy Act. I am the chief privacy officer, but I also hold the title of chief FOIA officer and given the situation with respect to Freedom of Information at the Department, I thought it prudent to do so to give greater visibility to the FOIA side because we have got a significant backlog and in fact over 40 percent of the federal government's backlog is the Department of Homeland Security.

We hired a Deputy Chief Freedom of Information officer who is also the director of disclosure, Catherine Papoi, who is here with us today.

We have advertised for and are in the selection process for a deputy chief privacy officer, and in addition we have created a new position, a director of Legislative and Regulatory Affairs.

The reason we did that was to cover one of the statutory mandates of Section 222 of the Homeland Security Act. We advertised and now the advertising is closed we are presently in the selection process.

We have also added two staff on the FOIA side of the house to help at the Department level with policy and with requests and appeals. I anticipate in the coming year we will commence work on the interim final FOIA rule to get that whipped into shape and out.

With respect to the committee, of course, we have had some folks who have come on board and there are some folks who are leaving us at the end of this year. I mentioned before that I anticipate a colleague of mine from Interior who is a federal advisory committee act expert will be available to join us on contract some time early next year.

I made the mistake of introducing him to the Homeland Security Advisory Committee and they snapped him up, so in his semi-retirement he has only so much time to give in a week and even if he is getting paid he doesn't have enough to come work for us as well, so we expect to see Bob Moll some time in early January, and I will be asking Bob to take a look at our charter and see if there are things that we ought to be changing.

This is not to worry you. I don't think there is anything, but as I did with the office, I want to do the same with the committee to look. We have been doing this for a few years now, so there are things that we can do to improve on what we're doing and in what you're doing, and of course, we will be working very closely with the chair and the vice chair on whatever we may be thinking about doing.

A subject that I had spoken about earlier this week with some of you is our quarterly meetings. I am inclined to move to a 50/50 split with two of our quarterly meetings held in Washington, D.C. and two being on the road.

My thinking is that site visits can be fun. I must say, although I have only one site visit under my belt which is far less as compared to all of you, but yesterday's was a phenomenal site visit not just from what we saw, but also from what we heard with the Coast Guard's willingness to talk to us about the ways in which they use information.

It was not just interesting, but also enlightening and I am very grateful that Admiral Nimmich had set that up for us. My thinking is, if we're in Washington, D.C., we probably can dispense with site visits unless there's something that's really critical that we need to see and we can spend more time on the committee's business.

But if we're out on the road where there are likely to be situations where we would not in our daily course of business have the opportunity to see or experience we would want to go out and do that.

In that regard, I look forward to hearing from you all on your thoughts on my suggestion. The work of the office. I would first like to mention has to do with our efforts, and in fact, Becky Richards' efforts, where Becky has a tremendous amount of work on her shoulders and does a fabulous job in getting that work accomplished as director of compliance.

On Citizenship and Immigration Services, and the U.S. Coast Guard, we have both visited to speak and we are in the process of getting their legacy system of records notices updated so that they reflect the changing situations and also the fact that they are no longer with their legacy agencies, but are now in the Department of Homeland Security and the admiral mentioned that earlier today.

PIAs are increasing and I anticipate, as I said the last time we met that we expect perhaps to see as many as 500 PIAs over the next year, or so, and as I have indicated when before you and elsewhere with 500 PIAs I could spend every working day for the next

year reading and signing PIAs, not even editing them and there wouldn't be much left for me to do.

We are therefore looking at ways to improve the work flow yet still make sure that all privacy impact assessments come up to the Department's privacy office. We are disinclined to delegate that responsibility to the components.

PNR. I am sure that many of you have followed what is in the news with our work with the Europeans on passenger name record data. I anticipate within the next month or so representatives from the Department, the Department of Justice, and probably the Department of State will be meeting with the Europeans in a high-level working group that was discussed at the recent ministerial EU/US ministerial.

The privacy office will be involved and I anticipate very strongly that I will be representing the privacy office in that high-level working group as we work with the Europeans to finalize the new agreement as we have worked past the interim agreement that is in place.

Now specific issues that I would like to talk to you about. First, is the annual report. I am very excited to say it's out. Unfortunately, we were unable to get our printing shop to get final copies for you, but we made some photocopies of the annual report and they are in the back of the room if you have not seen them or gotten them or been to our web site, so I urge you and those who are in audience to do so.

A couple of things to talk to you about with respect to the annual report. You will note that there is a one-page cover letter that is at the beginning of the report from me to Congress on the report.

It is not my report and I say that not because I want to distance myself from it, but because I want to acknowledge the hard work that Nuala O'Connor Kelly and Maureen Cooney put into this document, but were unable to get out during their tenures as privacy officer.

There is a lot of work that they put into it. When Maureen left, I read through it and looked to see what there was that we needed to do to get the document out. I thought it was a fabulous document and with the exception of removing appendices all of which were documents already –

MR. TEUFEL: That's interesting. Well, you have a lawyer talking, so it's hot air and no doubt the HVAC has to kick in.

As I was saying, the appendices were mostly if not completely documents that were already in the public domain and I thought in the interest of getting the report out in a timely fashion and in a cost-efficient manner that I would not include the appendices.

The next question I asked myself and the staff was, how do we go about getting documents out? Mindful of Congress' statement, no appropriate funds could be used to delay the report, and the President signed the statement saying, notwithstanding that language in the Appropriation Act, the president if he wanted to, could look at the document and make changes.

I do believe and support the concept of the unitary executive as does the administration. I think the HVAC has actually gotten louder.

The first thing I did was go to our executive secretary, and say, Would you put this report through the usual process? Even before that, I went to Toby Levin who you all know was a very senior and very respected career privacy official within the government in our office and I asked her to take the lead on any comments or suggestions or proposed edits to the document.

I did that because if we made changes some might say, "Hugo did you do that for political reasons", and having Toby there as a senior career employee it would be very difficult to make that assertion about her work with the editor's pen.

I should tell you that we went back and looked and we didn't have a lot of history because there had only been one report that had come out. We attempted to find out what had been done with that one report and it wasn't clear to me what the review process had been. Having worked with other independent was quasi-independent offices in the past my concern was, if we were too insular in our handling of the report that we would miss good things that other people could point out to us. We would have factual inaccuracies or worse we would be wrong in the positions that we have taken.

So I went to the executive secretary and I said, Please put this through the standard process, let's shorten the period of time and send out throughout the Department and let's see what we get back. We had very little if any in the way of substantive comments, but we had a lot of very good suggestions in terms of style and grammar, in the use of abbreviations in the names of particular offices and programs within the Department. Frankly, had we not done that we probably would be embarrassed because we would have gotten some things wrong.

So, we went through that process and when we were satisfied that we got it right, we were ready to go live with the report when somebody pointed out that the cover letter that was for Maureen, and Maureen had now long since been gone, so should we leave that document in there and our decision was that after some internal discussion with the Department, no, we need to acknowledge that we were late, and talk a little bit about why we were late and let folks know that this was not the incoming officer, but this was really the work of the previous officers.

So by way of that explanation, I wanted you to understand how we got this report out.

I anticipate next year's annual report will cover July to June should be out in a more timely fashion and with any luck we will have it out by September of next year, but I am pushing for about a two month turnaround in terms of review to get the report out to you all. That's the annual report.

Let me find my notes and then I will hit the other big issue that has been on our minds over the last several days including while I was on vacation in the Western Caribbean last week.

ATS. Yes, Automated Targeting System. Some points for you to know about ATS. ATS is associated with the Legacy Treasury Enforcement Communications System, but has sufficiently evolved enough that it probably needed its own system of records notice. ATS is not new. Customs had been using ATS for cargo since 1996 and for passengers since 1999.

The previous system of records notice that it fell under was the text system of records notice which first came out, I think, in 1978 or 1979, and then was modified in 1984, or in 1987, but we will have some folks from customs and border protection who will be coming up later.

He can correct me on the dates, but I think it was in 1987 that text was in its next iteration and the last revision to the text SORN was in October 2001.

The other thing I should note is this. Had DHS not come into existence and had this program still been over at the Department of Treasury probably it would not have received as much scrutiny as it has in the last week. This is not an excuse, but certainly it is understandable given the very broad scope of the mission of the Department of Homeland Security has that there would be great interest in what we're doing at the Department, and in particular, what Customs and Border Protection is doing to secure the homeland and to secure the borders of our country.

The system of records notice for ATS went out in early November with a deadline for comments of December 4th. We received a number of comments and some very good comments and we also received requests to extend the period of time for comments including from incoming committee Chair Bennie Thompson.

We looked at that internally and we said that there are some good reasons why we ought to extend the comment period not the least of which being the privacy impact assessment for ATS unfortunately came out some three weeks after the system of records notice came out.

One of the last things I did at the office Monday before getting out to prepare to come down here was to sign an extension to be published in, I believe, this Fridays Federal Register, extending the comment period until December 29.

Some areas of concern with respect to ATS that we have seen or heard and I want to highlight them for you. The first is the retention period of 40 years, which we know many of the commentators have taken issue with. In speaking with Custom and Border Protection it is our understanding that they view this as within law enforcement circles as the average period of time at which someone would be engaged in criminal activities over the course of their life.

Next is the use of the text exemptions to the Privacy Act. You will note that we have language talking about the possibility of reviewing those exemptions within 90 days. I do not want to get ahead of myself, but it would not surprise me if we do go and look at those exemptions especially after we have gotten the full compliment of comments on the system of records notice, so I would not be surprised if we go and review those exemptions.

The third area of concern that we have heard is the use of or the consideration and determination that PNR data is law enforcement data and therefore is exempt, so there is nothing else to add on that one as it is pretty straightforward.

With that, I have run out of steam and I leave the floor open to you for questions you might have for me in the time we have remaining.

CHAIRMAN BEALES: You have all turned up your tabs all at once and since I don't know who went first, we will start with Joanne McNabb.

COMMITTEE MEMBER MCNABB: Thank you. Hugo, I wonder if you could give us any prediction on when the Department will be issuing the REAL ID regulations.

MR. TEUFEL: I don't know but the answer is ... I am looking at Ken Mortensen and Becky Richards if they have heard anything more from Toby who has been working this issue very closely as you know because you have been working with her, if they have any more newer information than I do.

The answer has been the same for some time now. It is soon. I cannot be any more specific than that because I just don't know.

CHAIRMAN BEALES: Jim Harper.

COMMITTEE MEMBER HARPER: Maybe an addition to your list of concerns about ATS, there is language in the 2007 fiscal year appropriation for the Department of Homeland Security. I don't have that in front of me, but the gist of it is that no funds shall be used to create risk scoring of people who are not on a list of any kind.

That risk scoring has a lot of fairness concerns that motivated objections to secure flight. I know it is not your job to enforce the appropriations rules, but it needs to be taken cognizance of and the privacy office might help educate DHS folks as to why risk scoring of non-suspects is a concern.

MR. TEUFEL: For five years in my two previous jobs appropriations law was within my area of responsibility and even though I am no longer a practicing lawyer appropriations law is near and dear to my heart.

Whether it's risk scoring or our ability to have government funded coffee and donuts, I do take it very seriously because I know Congress does and the GAO does and if we were not to do so they would remind us in a number of ways where we need to take that stuff seriously. We had some internal discussions about that language, and yes, we will do our part within the Department to make sure that the Department complies with the law.

CHAIRMAN BEALES: Tara Lemmey.

COMMITTEE MEMBER Lemmey: I must say that I was very surprised when I learned about ATS in the news while I was in Hawaii and I was receiving e-mails from various friends and colleagues around world who knew I was on the committee and asked how much we had reviewed this and whether we had input.

It was difficult for me to say, as far as I was concerned, we did not really have a lot of conversation about this beforehand and we had not really known about it, perhaps maybe some other cargo aspects, but not the other aspects of it.

Your comments about the input so far seems to suggest that citizens' data being collected in there falls under criminal rules which is going to be an important area of discussion an on-going basis.

What I would like to know is what you think the role of the committee is and what our participation should be in the discussion of the guideline in going forward even though I would no longer be on the committee I know my colleagues will do an excellent job in helping the Department think about it. How do you see that role in going forward?

MR. TEUFEL: Let me say that I wasn't there, but I understand that you all saw it in use at the Boston Airport when you went on an on-site visit there and then also when you were at the National Targeting Center you may have seen it in use.

Again, I wasn't there. I have just been advised of that.

With respect to what the committee might do, frankly, I think given the posture of ATS and the program and the media and the congressional attention focused on it now it's probably past the point where there are things that the committee can do. It's already

out there. It is live and we have heard from Congress and we will be hearing from Congress.

I can see if we can go back some years to an earlier process or to an earlier period of time where ATS was not as evolved I could see that there probably would have been a number of things that the committee could do, but at this stage it has probably gotten too far.

I might be mistaken and certainly I will hear from you all either here or afterwards.

COMMITTEE MEMBER HARPER: Two follow ups on that. Although I was in Boston and although we may have briefly seen it, I don't think we were briefed on it and really understood the implications of it in any way especially with a 40-year retention with the notion when under criminal aspects.

I would like the committee to be on record, as far as I am concerned, I was there and I wasn't briefed. I don't know how my colleagues feel, but they seem to be in agreement.

MR. TEUFEL: I understand, but again, I wasn't there so I cannot respond.

COMMITTEE MEMBER HARPER: On the second point, as far as the role of the committee it is important to recognize that some of the leading experts in the world on privacy are on the committee and that their engagement should be considered on an ongoing forward basis because the technology aspects of privacy as the technology advances is absolutely critical, so I think while you may be reviewing the current set of operations you should think about this on an evolving basis and there may be a place where the committee could be involved and I certainly urge you to have the committee participate in some way.

MR. TEUFEL: That is a good point and thank you very much.

CHAIRMAN BEALES: Let me add that it's fair to say that we were not briefed on this system in Boston, that is right, but we saw it in operation.

It was clear as to what kinds of information were being used, what kinds of determinations were being made based on that information, and what kinds of consequences were followed from those decisions.

I never knew the name, but when I heard the first stories, I said, Oh, that is the system we saw in Boston, because that's exactly what it was and how it was described and how it was presented.

I will say that I think there is a lot of value in PIAs and the SORN requirement is transparency. That is certainly much greater transparency than has been achieved here.

MR. TEUFEL: Yes.

CHAIRMAN BEALES: By doing this.

COMMITTEE MEMBER HARPER: I would like to make the recommendation then for the on-going site visits is to perhaps have the PIAs available for the systems that are being reviewed by the committee so that it can be looked at in context as opposed to maybe considering what the short term aspects are, but not really looking at the details of the underlying system.

CHAIRMAN BEALES: That is a great idea, but one of the difficulties here is that it has been very difficult to get a PIA produced on a program that has been in existence for a long period of time.

I personally appreciate the Privacy Office's efforts in getting these documents out so that we can see more clearly exactly what it is and exactly how it works as that is the point of these requirements and when they are there we ought to use them as part of those programs and I think that's right.

MR. TEUFEL: If I may interject and note that we did so with them on a past PIA this time around.

I wasn't there, but we wouldn't have been able to have done so previously because we did not have a PIA out until November 24th of this year.

I am looking over there to get the date. I am just remembering how much fun it was around Thanksgiving to get that document out ... was a struggle.

If you will forgive me there are very few calls I take, my wife and the secretary, and this time it is not my wife. I will have to come back and we can discuss this a little more, but I have a phone call to take.

CHAIRMAN BEALES: Thank you very much, Hugo, we appreciate your being with us today.

Next on our agenda is Mr. Peter Pietra from the Transportation Security Administration.

Peter was named director of privacy policy and compliance at TSA in April 2006 after two years as the head of TSA's information law office. Prior to his service at TSA, Peter practiced law in Delaware on insurance, intellectual property, and construction matters, which I am sure have a great deal in common. He has served on active duty as a field artillery officer with the Army and as a lawyer with the Coast Guard. Peter is a graduate of the University of Pennsylvania and Temple University School of Law. Peter, welcome.

MR. PIETRA: Thank you very much for inviting me to come here. I was telling Richard earlier that last week I was in Colorado Springs and when I left it was 12 degrees,

so I was happy to hear that I was coming to Miami this week, and I want to thank him for that although he is not here.

What Becky suggested to me on what you might want to hear from me was basically what we have been doing for the last seven months at TSA in privacy and in the privacy area. So I made a list of projects that we have done, and about some initiatives that we're trying to implement in going forward and at the end I will be happy to take questions.

I will be very happy to take any suggestions on matters that you think we should try to focus on in trying to build a program that's more useful to an agency.

We have a little over 50,000 employees at more than 400 locations, so one of the biggest issues that I see, and what is one of the largest and constant efforts that we have to undertake, is obvious. It is education.

That is a fundamental point, but when you have people who are spread out in so many different places who are doing so many different tasks, that if you do not get the word out, and they may not realize it even when you do get the word out, sometimes they do not make the translation between the privacy principle and what it is that they are actually doing.

For instance, take a contact list that I may have of industry officials. It is technically something that would be covered by a PIA under the E-Government Act, but how different is that from my contact list in Outlook and why is it that I would have to do it for this one but not for that one? So this is something that might be overlooked but we're actually struggling with right now even though it is only business information.

We've done a number broadcasts that have gone to all employees, including every screener. They have limited access, but they do all have e-mail accounts and they do have access to computers out there at airports.

We have covered a variety of different topics. The first one I sent out actually came out of a case out of the Department of Health and Human Services as an EEO case that had to do with checking who is on your distribution list before you send out an e-mail. So check that every single person who is on that e-mail distribution has a need, even a second-level supervisor, before they get that information.

That was the very first one we sent out and since then we have sent out broadcasts on protecting personal information that leaves a TSA facility. Certainly in the aftermath of the Veterans Affairs incident this summer, and there have been lots of other data losses that have been suffered by both government and the private industry, so that's a real issue and it is one that we want to get the word out on as to exactly what it is that TSA is going to require.

We sent out a broadcast on training, with the need to get it done, which is one of the things that has well, I will not say has languished, but as people are taking the training, there is an enforcement effort on catching those who have not taken their training within the 30 days when they first started with the agency. So we have reinvigorated that process of going after the people who just failed to get around taking their training.

We did a broadcast on protecting metadata when you post things to the web. I understand that there have been instances where people will use a spreadsheet or something else on an Intranet web site or on an Internet web site, and if you manipulate a document then some times you find lots and lots of hidden columns that you wouldn't have thought were there. So we wrote up a policy on that and now we have a way to scrub all of that information before it ever gets posted on the TSA web sites.

Another broadcast that has become routine is to be aware of phishing. I've gotten different efforts that were directed to me including updating my Amazon account as well as to update various credit cards which I did not have, and there was one very official looking one from the IRS, which promised me that I would get a tax refund; I know I owed taxes so a refund email was a surprise.

We have targeted messages to specific audiences where we have had issues that are specific to airports using a broadcast system that's directed straight to the federal security directors at the airports. We did a broadcast having to do with their use of their own employee rosters and how they're handling them. I have also used my old field counsel chain from my prior position to pass the same message, but put in a little more detail so lawyers at airports can provide advice to their leadership at the airport.

We have done a Privacy Awareness Press. Tony Johnson, somebody who I stole away from the Coast Guard, who was a privacy officer there and is now working with our office, is bringing out on a monthly basis a kind of a sampling of what he has viewed to be privacy issues of interest to the press which may help to illuminate what are the issues that the public is concerned with so that our managers will understand without my having to tell them, for example, that if you do risk scoring, that's something that will be a concern. And we will think long and hard before we ever try to go down that road again.

In addition we just have a general constant interaction with managers at headquarters and out in the field that's a constant, but with this far flung kind of operation that we have, outreach is something that we have to do.

Privacy training. One of the first things I was asked to do when I came on board back in June was to really get after the training to make sure that we got all of compliance numbers up. So that the people who had failed to take theirs in the first three days, there was a consequence where we were going to go after their leadership telling them, You

have to take this training and get this done. The numbers have gone way up from 90 percent compliance in July to 94 percent in November, so it is creeping up which is something that we are very happy to see.

We have also done "Privacy 101's" with certain teams within our assessment community and within our leadership just to give them a half hour, 20 minutes showing, "This is what it's all about. This is how a SORN works with a PIA." These are things you need to think about before initiating your program or when you're making changes to your program.

In terms of what we produced, we have published seven PIAs since April. We have three more that are up for review and we have about twelve more that are in the works. The ones we have published since April have covered port access, which was a precursor to TWIC. It's not related to TWIC, but it's intended to get at assessing some port workers so we had kind of a sense of, Yes, this is a real problem, or, No, there is no real problem. So until we get TWIC up and running we published this port access PIA.

We have done the TWIC NPRM PIA. We did one for air cargo. One for our own visitor management system in terms of our TSA facilities. One for our redress office. We have done the next phase of Registered Traveler, and we did one for a Hotel Access Pilot down at Dallas/Fort Worth eventually to cover a program that would allow guests of hotels who are co-located within the airport to access into the secure area to go shopping or to go to their restaurants, so if you're stuck at an airport you can go into the secure areas. That started just last week.

We established a web site that is at www.TSA.gov/privacy and I will admit that it is not visually exciting. Mostly that is my fault, but I am hoping to try to make it better over time and as we are able to devote time to it.

What I have put on there, though, are some basic FAQ's that cover some of our programs, some of the things that we have seen that people have been curious about, so it handles matters such as, "I get stopped every time I go to an airport, does that mean I'm on the watch list?" It's those kinds of things.

We also put in links to all of our PIAs and we have put in some links to the DHS privacy office. We put in a link to our Redress Office, to our FOIA office. If people do have an interest in privacy, as I said the web site is not fantastic, it doesn't have games to play, but at least it has the basics in terms of if you want to get some FAQ's you can get an answer to a question that really will affect you, you will be able to get it there.

There's also a section there for government employees that provides a link for training, for example, and we were considering whether to add system of records notices and a separate kind of employee Privacy 101 that says, This is the nitty gritty and if you're

an employee, then these would be the kinds of things that you can expect to face and how to handle those.

In terms of policy development, we did write a policy on PII leaving a TSA facility. It does not cover all PII because I felt it would be too unwieldy to do that, but we cover every record that has a name that's combined with one or more of a bunch of different items. So if it is a name that's combined with a Social Security, or with a date of birth, or passwords, or medical information, EFT information, financial information, if it is that sort of thing, that's covered by the policy and you cannot take that out of the facility. So you cannot work on it at home and you cannot take it with you as a hard copy or electronic unless you've protected it. I don't want to hear or find out that an employee has taken a hard copy list of records then left it in their car and then it gets stolen or maybe it's a laptop or a thumb drive, any of those kinds of things. They are required to be encrypted now and we want all electronic devices to be secured. If you're teleworking from home, it has to be on an approved schedule and it has to be on a VPN. That policy went out November 1st.

As far as staffing, I hired Tony who was with the Coast Guard so at least he's still working within the Department.

We also developed a privacy system review to try to match up and confirm that our programs SORNS and PIAs accurately cover what it is the program is doing so that a year after the PIA is out they are not doing something different than what we said we were doing a year ago. If they're going to make changes in the future, then we can kind of anticipate those and try to get on the ball in terms of deciding, first, whether these are good changes, and second, if the documents that we have are accurate and they reflect or permit what it is they want to do.

The other benefit of that privacy system review is that managers change, so a lot of times you find out that program management has changed and the first time you find out about it is when you send the documents to the old program manager. The new one may need more intensive privacy education, as well to understand exactly how the program works. So that's another benefit, and I am hoping this will do. We have five systems reviewed so far, and in some of them we have found some differences. This may not sound significant, but in some cases for example, there is actually less information collected than what we had anticipated when we wrote the PIA. So that's been a helpful process.

I also wrote a more formal kind of compliance audit than the system review, but I haven't used it yet, so we will see whether it is a good audit or not.

Things that are coming in terms of policies, and I talked to Joanne at the last meeting on something I sent to her, and that is in all our contracts we have standard

language for privacy, and certainly if we find out about a performance problem, then at least I have been sending that information to the contracting officer so that when year-end performance reviews are done, they will have that information and they will be able to use that in evaluating the company.

What we don't have, and apparently no agencies have, is an up front kind of process to really evaluate, and require the bidders on a contract to address, privacy issues. So I put together a list of the factors that I thought were for the performance of a contract, and I am hoping within the next couple of months to fine tune that more, and insert that into all of our RFP processes so that when a bidder bids on a contract they will have to address specifically what it is that they have in place for protecting privacy and how they handle the contract, and that means people and policies and training and IT security.

I have been working a lot with our Chief Information Security Officer (CISO). We have very similar issues in terms of data security on our systems and that is just a matter of trying to cultivate and work with them more closely. So when I was in Colorado Springs last week, we have our operations center there, and our CISO came along with me to take a look at what it was the center was doing.

We're looking to reduce our dependence on the Social Security number internal to TSA. It's a very difficult process to try to break people from using that as the identifier and so I don't have a good answer, I don't have a document yet, but this is something that we're working on. One of the things we pointed out is that our employee badge has a number on it. So why can't we use that as the employee's ID number instead of a Social Security number? Right now the problem is that the systems are not tied together that way internally. There are some things where we do need to have social security numbers for, typically with pay which is near and dear to everybody's heart.

We are going to develop a breach response team. Right now, basically, it all comes to me and I work with CISO. There are the two that we have had so far, at least that I know about, but we need to have a more formal team. That is something that we will develop.

I will now talk a little bit about some of our high-profile programs and then we can turn over to you for questions that you may have in terms of where things are.

For RT, last week, the providers were enabled to begin pulling in information for program participants and they were entitled to start the enrollment verification process. None of them are ready yet to actually start transmitting data to TSA. My understanding is that the RT program right now is going to be rolled out in seven airports and one air carrier, since those providers are really ready to get that up and running. It is a market-driven program and it is a private sector program and TSA's involvement in it really is the vetting piece of the program. That's about it.

In terms of the benefits to the participants, some airports that will have the front of the line kind of privileges and providers will want to provide concierge services or links to auto rentals. There are things in the private sector that people want to provide that really we have nothing to do with. We have required that the data that is on the card is a stand-alone for our purposes and then the rest of it, as I say, they can do anything they want to do but they have to specifically tell the public, This is not something the government wants or what the government requires, or anything else like that, but is something they're doing independently.

There is a web site, a TSA web site which is a much better site than is mine, for Registered Traveler, that has quite a bit of information on IT and privacy standards that we are requiring providers to follow, how the program runs and who are the approved enrollment providers now.

In TWIC, the program was intended to test a common access credential that would be used with various transportation modes where this started off with the ports, but it's now a little broader than that and it will positively tie the person to the credential in their hand. The process would be at least to put a finger on a reader, put in the card and then type in a pin. We have had a lot of comments saying that that process was too burdensome, that they could not handle the throughput, that the cards were not going to withstand a maritime environment. What we're looking at now is doing a contactless card and now we're trying out a contactless process where it will still have a fingerprint, but you will not have to do the pin, so maybe that will address some of the other concerns from industry and others.

That's a process that will be taking some time and there are security concerns with this, so I don't have any sense on where that is or how well that is going, but that's basically where we are in TWIC. We are working with the DHS National Maritime Security Advisory Committee on a security specification for port contact and the data that is going to be transmitted is the name and a fingerprint template, not the fingerprint itself but a template. The program has received some criticism from the GAO and from the IG on program management, on budgeting issues for the most part, and things like that, so the program has hired some new staff to address those issues and they are working on those issues that were identified by Congress.

Backscatter was in the news last week, I guess along with ATS, and it got what I think was very unfair press in terms of the photograph that was shown. That photograph is not even close to what has actually been used and if you go to our web site you can actually see what it is and it's almost really an outline of an individual and then the items would show up. We have worked for more than a year trying to tone down the image so that it was not basically a strip search by turning it into more of this outline. We have

given up some detail, but it's been in recognition of the fact that they cannot do a strip search for every single person who comes through.

The technology is very good in terms of privacy. The screener that sees the person coming through is separate from the screener who is looking at the image, and the person who is looking at the image is remote, so if they see someone who is a TV star or somebody else who is coming through the checkpoint, the screener looking at the image cannot engage a prurient interest because they are just two completely separated.

Their images are not stored in the system. You can walk into the system and once any anomalies are resolved, before the next person can come in, the images are cleared and that's it. There is no print capability. So those articles that said that we're going to find images of you naked for years on the Internet, it's just physically impossible to do. I think this is a pretty good program and it will be hard to find concerns, so we will see how the pilot shakes out and I think it is a very good program.

Secure flight. Congress has directed us to take over the name matching function that the airlines currently undertake and that is all Secure Flight is. It does not access commercial data and it doesn't do the scoring. I don't recall if that appropriation language is limited to Secure Flight or if that is DHS wide, so I will have to take a look.

We are working with CBP to try and coordinate the data feeds so that the airlines don't have to worry about supplying different information for different government agencies and we are looking at what filters to put in place in terms of data that at the TSA we don't believe need or want.

That's about it. There's been the effort of the office so far to become an office that people who are looking for practical and prompt advice can get it, and that by being vigorous with more activities we will get more and more business in the future.

It's a double-edge sword, really, because if you're active, then you kind of get what you deserve and that means you get more business, but this is the best way for us to accomplish the mission of our office.

Thank you very much and if there are now any questions...

CHAIRMAN BEALES: Thank you, Peter. I thank Jim for his sticking around from the last time, so Jim Harper gets to go first.

COMMITTEE MEMBER HARPER: If there's time I would like to have a second question. I have a great story about the Liquids Rule that I want to use.

There was something you said that raises a more important issue to me. The registered traveler private sector initiative is something that I am very interested in particular because the Clear Card that is used in Orlando is capable of proving to the TSA

that the person is a member of RT without telling TSA who it is, so it provides an appropriate credential without using identification.

That is a remarkable and an important example of digital identity management which will become more important as we go forward society wide.

I have been aware as there are different multiple providers that offer cards and install kiosks in airports they have to interact with all providers where each provider's kiosks will interact with each provider's cards and vice versa.

For a time the interchange between providers may have run using personal information about travelers where it might say, Jim Harper, and there's a code obviously, but it might say, Jim Harper used the Clear Card kiosks in New Jersey and wherever else, so then they would reimburse one another that is running on top of personal information.

The Clear folks have a very clear privacy policy wherein they do not maintain personal information and they do not share personal information which is obviously a threat to what they were offering the public in terms of their offerings.

Now, I do not know is the status of that issue right now, but I think it's an important one for you to look at to make sure, for the purposes of the system, the multiple providers who operate on the same system that there should be a separate data channel rather than using the data about who uses which kiosks, a separate data channel that allows the providers to do what you might call interchange as far as who has used what kiosks.

There's no question there. I just wanted to encourage you to help make sure that the privacy protections now being offered in Orlando with the Registered Traveler pilot are available to any implementation of registered travelers elsewhere.

MR. PIETRA: Yes, I would be happy to look into that, but I am sure it's been addressed already. I don't know the specific answer. I do know that the pilot in Orlando that the company that is behind that is a very aggressive company on privacy and they really have strongly marketed their privacy. They have been involved intimately with every bit of decisions making in the RT consortium with all the industry groups involved and with those companies that plan to be involved, so I am sure they addressed that issue, but I will take a look at that.

CHAIRMAN BEALES: Joe Leo.

COMMITTEE MEMBER LEO: Thank you. I would like to pursue a question and hopefully maybe get a response that will enlighten me as well as the committee members a little bit on the credentialing program with regard to the Department's overall credentialing program because I am one member who is sort of confused.

I watched a recent TWIC controversy at the ports as to the costs and the expense and the reexamination of that card technology at the ports.

I am aware of Homeland Security directive 12 with regard to the controversy of costs and issues with that credentialing program and the fact that the ports do not have the funds, I am confused a little bit about how the technology ties into the U.S. VISIT Program that is going to use the ten fingerprint to be compatible with the FBI, so that's now all united, then somehow failed to find a vision of credentialing within TSA or the Department as a whole on how there's a better way you all are looking at this credentialing so that there's some not only cost savings but privacy protection and data integrity and so forth.

That is my general question to you.

MR. PIETRA: Sure. In terms of the data protections and the privacy issues, those are being addressed as each card comes up. The gravamen of the question is: Why is it that we're looking at all different kinds of credentials?

My understanding is that it is in part because cards operate in very different operating environments. The U.S. VISIT program has fixed readers. They have got data entry points that are quite different than the TWIC card which in many cases, well almost, but not in every case, do not have fixed readers and the TWIC card has to perform - Well, the TWIC card doesn't give you access to a facility, the TWIC card just says that you are the person who you say you are and that is all it does. The facility operator actually will set it whether or not you have access. Whereas, with VISIT, as I understand it, and I cannot speak for VISIT, but my understanding of VISIT is that it grants you access to the point.

RT, I think is closer to the VISIT model than the TWIC model.

That's the long way of saying I cannot give you a good answer on that and what the thinking has been and why is it like that as it seems to be different credentials for different programs that are run by the same agency.

COMMITTEE MEMBER LEO: I did add one more which was HSPD-12 because that requires that all federal employees have this new standard and all federal contractors that provide services, where a contractor that provides contracting services to the government, and as you know there are a lot of feds in airports that are this or that, so I am trying to envision all of these credentials within the same community.

That was the genesis or the purpose of my question.

MR. PIETRA: It is a good question but I am sorry I don't have a good answer for you.

CHAIRMAN BEALES: Charles Palmer.

COMMITTEE MEMBER PALMER: We all know that x-ray systems are adjustable up to a point and in some situations your shoes might set it off and with others they may not. My curiosity as a technology person is, of course, about the back scatter. How adjustable is it? Will it be capable of adjustment in the field, and if so, could the system be reconfigured to provide more or less detail than your web site pictures would imply?

MR. PIETRA: Obviously, it's adjustable because of the images we had from a year ago are very different than what we have today, but I don't know that it is adjustable at the field location.

I am also very confident that given the year of work that we have put into developing the image that we have now, and this is an image and a level of view that was mandated by Kip Hawley, our administrator, this is not something that will change in the future.

I don't know what else I can really say to make it a guarantee, but because this has been examined so closely so carefully with so much work, time, and money that's been put into coming up with the images that you do see now, I am as confident as I possibly can be that what you see on our web site now is what's going to be used now and it is going to be used in the future.

COMMITTEE MEMBER PALMER: The only reason I ask is because some my colleagues have looked at voting machines, for example, that shouldn't have been field programmable and were found to be. So I certainly hope these things will be looked into. Thank you.

CHAIRMAN BEALES: We have time for one last question and then that's Larry Ponemon.

COMMITTEE MEMBER PONEMON: Thank you. I really appreciate your responsiveness to our questions. This is just a general question about the architecture, if you will, of the privacy programs at TSA which is something that Joe was alluding to.

It seems that the news, the media, they find a story almost once every month or every week on some issue that involves TSA in not doing privacy right or in not protecting the privacy interests of the public. If that's true, it would seem to me that there is a need for an overarching strategy in privacy at TSA. So is that your role?

Do you envision your role, say, as you get to all of these compliance issues and training people internally and protecting data internally, do you see your role or someone's role as built in privacy strategy? Now, the reason why that is important is this. At our last meeting Michael Jackson mentioned that privacy is actually baked in. I am using my own words. But it is baked into all TSA programs and it sounded really good to me.

I think its great and I have a lot of respect, by the way, for what you do at TSA because it just a very, very difficult job, but at the end of the day who is actually building that strategy, that over arching privacy strategy, so therefore to be identity, credentialing, and vetting programs, they all have kind of a common framework from which you can start to build out solutions.

MR. PIETRA: Yes, that's my job. I don't know that there is a news story every week and I don't think I am being Pollyannaish here. You cannot separate out the compliance portion of what we do and the strategy.

My official title is director of privacy, policy and compliance because they are so interwoven because if you do not do the compliance things where we have to do the PIAs and privacy training, the SORNS, the paperwork reduction applications, if you do not do those things and have the kind of interaction that those things entail with people who are deep down in the weeds in the program, then the word is not going to get out that there are privacy issues that you have to think about and address.

I do work with and we have someone in our office who does work with the people who are looking at the checkpoint of the future, people that are looking at what other technologies we want to make, so there are things that I haven't talked about today that we do in terms of the long term goals of the agency to try to make sure that people understand privacy. If it's your thought of using RFID as people walk through the airport to adjust the way that the magnetometers read, it implicates privacy so you need to think about that and here is what we see as being specific problems.

One of the things that annoys me is when people say, Well, you have privacy issues, but they don't say what they are exactly. That does drive me crazy. So I try to become very particular with the advice that I give to our programs.

Now do I have an overall strategy other than the things that I have talked about in terms of really doing outreach and really trying to make sure that people are doing the right thing, I would say no. Are these issues that Joe raised about a common card an issue that we were talking about, yes, and it is not just that. Our threat assessments vary across our programs and in some cases they are driven by Congress which is kind of an historical artifact with that, so that program has a very specific threat assessment and other programs have different components to that.

The new TTAC program that Stephanie Rowe is looking at is shifting the structure of the threat assessment office from kind of a program centric view to more of a functional view so that in the future our threat assessments will be a term of art almost where it will have a specific meaning, and I am working with her right now on doing that exactly that to try to come up with, to the extent we are able to, given the outside influences that may have influenced the design now. And credentialing is along the same lines.

As I said at the very beginning, it's been seven months so I am not really that new on the job, and prior to that I dealt with privacy for two and a half years when I was with the chief counsel's office, but I am very happy to take any kind of suggestions on what you think I ought to be doing, where if you had an agency that was spread out with 50,000 plus employees, what is it that would be a priority to work on?

Obviously this is something you have to build in when you have lots of other things to work on, but the Social Security number is a policy where we are reducing that use, which is something that every agency does and what lots of private employers do, so that is a policy initiative that we want to work on that is strategic. Yes, we made the decision that we want get away from that. We said we're going to come up with something, but that hasn't happened yet. We are working with OPM, but we're trying to get out and get ahead of that.

COMMITTEE MEMBER PONEMON: I appreciate your thoughts and your responses and I do look forward to working with you.

CHAIRMAN BEALES: Peter, thank you very much for being with us today. We really appreciate your time and your answers to our questions.

This is a group that I am sure is full of suggestions so you may regret you asked.

Our next speaker Mr. John Wagner who is director the passenger automation programs in the office of field operations for the U.S. Custom and Border Protection Agency.

He joined the U.S. Customs Service in 1991 as a custom inspector in the New York New Jersey seaport. He also worked as a customs inspector for six years in Laredo, Texas on the US/Mexico land border. He has been assigned to headquarters since 1999. Mr. Wagner has responsibility for the International Trusted Traveler programs, for the Advanced Passenger Information System for the Western Hemisphere Travel Initiative, which I think is mostly what we are going to hear about today and various biometric technology programs including close coordination of the U.S. Visit Program Office at DHS.

He is accompanied by Larry Castelli who is the chief of Privacy Act Policy and Procedures in the office of Rules and Regulations at CBP.

Mr. Wagner, Mr. Castelli, thank you for joining us.

MR. WAGNER: Thank you for the opportunity to be here today and we thank you for the time on your agenda to update you on one of the more significant programs that the Homeland Department is working on.

I timed that perfectly.

The western hemisphere travel initiative, WHTI is what we like to call it, is a pretty significant undertaking by our department and the Department of State. I want to take time today to update you quickly on where it is we have been and what progress we're making in the process and give you some of the insight on how we came to some of our decisions.

Let me talk a little bit about why we think we are doing things right and why these are some of the avenues that the government should take to implement these requirements. This was a requirement that came out of the Intelligence Reform and Terrorism Prevention Act of 2004. What this requires is a passport or other alternative-type travel document of people whose passport requirement had previously been waived and that generally narrowed down to American, Canadian and Bahamian citizens who are traveling within the western hemisphere.

The way it is right now travelers in these categories can go within the western hemisphere with no standardized travel document and in a lot of cases they have no documents at all, so it is very difficult for us at Customs and Border Protection to confirm somebody's identity, to confirm their admissibility into the United States and do an accurate check of them against the watch list and with the other databases that we rely on.

We believe it's really important that people have some standardized travel document that we can quickly read and quickly validate upon their arrival in the United States.

We are looking for things to do quickly with this because we just don't move through airports, we don't like to stand in line, we just don't have the time with the amount of traffic that we have and with the amount of passengers, so we do not have the time to sift through different documentation, the 8,000 different birth certificates that are there, the 50 different state driver's licenses, we just cannot be experts on all of these different documents.

We just don't have the access or the systems just don't exist to confirm the validity of a lot of those documents to determine who is really holding them.

We are looking to this initiative to close a lot of those security gaps and give us the ability to quickly and accurately identify people, and in essence, what that does is to expedite the movement of the great majority of the travelers who we do encounter each day.

We do process over one million passengers a day who come into the United States. This is crucial. By just adding five, ten, or twenty seconds to each one of our inspections of those people has a dramatic impact on the rest of those people who are waiting in line and it has a snowball effect on the clearing out of a lot of that traffic.

So we're putting a lot of thought into what are the right documents that we want for this mission. We just recently completed the rule making process for air travel and the regulation goes into effect January 23, 2007, and we just published the final rule on that. It basically says that everyone has to have a passport for air travel into the United States. The two notable exceptions are the Nexus Air Card when using the Nexus program and the U.S. Coast Guard issue, the merchant mariner's document, the Z Card, for travelers who are traveling in conjunction with official maritime business or on ship's business that we do not see too much in the air environment, but it is possible that this could happen, so we put it in there.

Our current analysis of the situation right now shows that 90 percent of air travelers between the United States and Canada, and this is mainly who this will impact, over 90 percent of our travelers are already using a passport today. So when this does go into the effect on January 23, we will be looking at those percentages, and as this increases, we will look at how strict we enforce those so that there will be some period of flexibility that we will have as we go forward with this.

There is some transition period. We just don't want to use that date and cut off travel or significantly impact the way things are operating. We will be carefully monitoring these and we will take a pretty strong and quick definitive action and we are confident that a lot of people are and will be complying with us.

With that, moving to the more difficult portion of the rule making, that is the land and sea rule. There was some legislation in our appropriation act this year that pushed the land and sea implementation date back to June 1, 2009, or three months after Homeland Security and the Department of State certified that certain conditions are met.

The most significant one is the miscertification, the Pass Card, which I will talk about in a few minutes, that that architecture meets or it exceeds ISO security standards and meets the best available practices for the protection of personal identification documents. I will tell you that our goal is not to wait to June 1, 2009. We would like to get this out as soon as January 2008 which is a full year and a half ahead of schedule. We do recognize that this is a significant challenge for us and we have a lot of work that is ahead of us to do this.

We are in the process of crafting a notice of proposal for rule making for the land and sea environments and this will cover all of our land border crossings, all of our different methods of sea travel by cruise ships, small boats, charter boats, by commercial vessels carrying cargo and commercial merchandise, and it will also identify which specific documents we looked at and why we would approve or not oppose their use in these different environments.

We are looking at the Pass Card, our Trusted Traveler Card, the Fast Nexus and Century which I will talk about in a few minutes too, our border crossing cards, the legal permanent resident card that's out there and the Native American tribal documents that are also in use.

Some of these are outside the scope of the WHTI legislation. So with some of these, the experts and the lawyers are looking at to tell us which ones we still have to accept because they might be outside the scope of what this requirement is imposing. We will also be looking at driver's licenses and birth certificates and whether those have a use at the land or sea ports and whether they do reasonably identify a person's identity and citizenship and what is our ability to confirm that these are accurate and true.

So keep an eye out for PNR for targeting that out early next year that will probably be, I will just throw this out, I will say the March/April time frame. It is still in the process of being drafted and we are still looking at the initial policy decisions on how it is going to be.

The land border process, as it is today, it is a challenging environment. I spent several years down at the Mexican border working there and I can tell you that you never know what you're going to see in a car when it comes out of Mexico.

In an open trunk, you can find just about anything or anyone in there. You never know. We get no advance notice of who is coming or who is in a car which is unlike our airports and our seaports where you have AFIS, and the PNR where we have some indication of who is on already on board the planes who have already gone through a security screening process before they boarded that plane overseas, so that we have hours of notice in most cases of who is on board those planes so we can do our targeting in advance.

We don't have that with our land borders. People just show up. There are places like Arizona or Mexico where the border might be a couple of feet away where they can jump back and forth all day long, so you just never know what or who will present itself in front of you.

What we're looking to with this initiative is to have documents that we can read and confirm at that primary inspection point. We're looking for a document where if we have ability to do it 20 to 30 feet in front of the primary inspection booth that's what we're looking to do.

It has a facilitation benefit and it also has got an officer's safety benefit for us. The solicitation benefit is one where we can at least identify a person, run their information against the watch list as they're pulling up to the booth because we have all the information that was already presented to us that's in front of us by the time person has arrived and we can quickly clear them through the inspection process.

The officer's safety angle is this. The last thing you want to do is to take somebody's ID, turn around and run it through the computer and turn back around and find out who they are and find out they have a warrant outstanding for their arrest that is also saying they are a dangerous fugitive or a dangerous felon.

That is a reality.

People do get hurt. People get killed on this job. So if we can have the ability to at least give the officer 20 or 30 feet of advanced notice that this person who is about to approach them is a dangerous person, they can then take the appropriate action to not only defend themselves but the rest of traveling public who are around.

This is a dangerous environment to work in. So this is an important benefit.

What we have had pretty good success with is the Trusted Traveler programs or the Registered Traveler programs. We have Century that is on the southern border. We have the Nexus program on the northern border and then the Fast program for commercial truck drivers on both borders.

These programs go back to the mid 1990s. Century goes back to 1995. What we saw was where we have border communities there is a commuting population that go back and forth all the time, going to school, to work, just to visit friends, just to go shopping and some people cross multiple times a week and even multiple times a day.

So we're looking for a system, when we have to see this person every single day, and ask them the same exact questions each and every day when we already know they are a United States citizen or they are a Mexican citizen with a visa or they are a Canadian citizen, but we have to ask that question of them every single day.

So what we devised over time was the RFID enabled card. We have the individual fill out the application. This is all on a voluntary basis. They fill out an application telling us who they are, where they live, where they work, and we run that information through the various databases, we run criminal history checks and then we bring the person in for an interview being the same type of interview we do at the primary inspection point that confirms who they are, that confirms their admissibility into the United States and we also run fingerprints through the FBI to make sure there is no criminal history of the individual.

If they pass all of these tests, as far as the RFID enabled card, the next time they drive up to the border the reader will read the card and their database record will appear on our screen at which time we run a cursory run on them before they get there so that we can expedite their inspection.

What we're doing is we're calling up the results of that pre-inspection that we had already done on them and the RFID only transmits a final number. That's the only thing that is read. There is no battery in this card. It is the passive type I believe.

There is no battery. It is just a number on there and the reader picks it up and that corresponding file in our government's secure encrypted database that appears on our screen and we can compare the picture that we have of the traveler that we took during the enrollment process and the results of the queries we need to run with the person in front of us and then we can expedite their inspection.

What we do is we give them dedicated or exclusive lanes to use for coming back and forth when using this program.

The Nexus and Fast program along the northern border are done jointly with the Canadian government and the Canadian government also performs a similar risk assessment of each person. You have to get approval by both countries to participate in that program.

We have made one application in which the person submits to both governments and we collect the fee one time and split it and we have also built-joint enrollment centers so you get interviewed by both governments at the same time for more of a convenience type benefit.

We have had a lot of success with these programs and I do believe about 5 percent of our overall land border traffic is crossing through these programs right now.

We have about 275,000 people who are enrolled in these programs.

Some places like in Blaine, Washington, nearly 10 percent of the traffic is coming through those Nexus lanes.

We considered this traffic low risk which is a huge benefit for us because it allows us to focus on people who we don't know anything about, the high-risk travelers, so we focus our resources on those lanes while we are expediting people across the border all the time.

We looked at this Fast, Nexus and Century Trusted Traveler card concept and the way the IT system works and we feel this is the right approach to take with the Fast card which is the card the Department of State wants to issue for the lower-cost passport alternative for land border and seaport use.

We are looking at the same type of architecture that the State Department will issue a card based on how they issue a passport today, but it will have this RFID with a device in it that will allow us to call up that record when a person is pulling up to the border.

Again, this is just a file number that's being transmitted. There's no personal data of the person. It allows us to identify the person, run the watch list query on what we need to do and it also confirms that the document that the person is holding is a valid document.

We can then compare those in the database against the person who is presenting it and then make the determination that it is the person that they are admissible into the United States and we can then let them go through.

We feel pretty strongly that this will have a facilitation benefit and an enforcement benefit because we will be identifying people who do come into the United States which is something that we struggle with today, and quite frankly we take a lot of criticism today because we don't have the ability to query land passengers against the watch list.

The amount of traffic that we are faced with each day with the time constraints it just doesn't allow us to do that to have everyone come in and we type their name and compare them against the watch list.

This is important for us and we feel this is the right way to do it. That is a quick overall snapshot of at where we are at with the WHTI program. So let's open it up now for any questions and I will do my best to answer any ATS related questions as well. I am not an expert on that, but I do have some visibility into it, but Larry is here who proclaims to be the expert.

CHAIRMAN BEALES: Thank you very much, John. The first question will go to Dave Hoffman.

COMMITTEE MEMBER HOFFMAN: Thank you very much. I want to ask you a bit more about the deployment -- Sorry? Do you need me to speak louder?

MS. RICHARDS: Yes, we are losing you because of the air conditioner.

COMMITTEE MEMBER HOFFMAN: I would like to talk a little bit about the deployment of the RFID technology and its implementations that you are using, but I continue to be confused by it. I have seen the implementation of it at the border in Blaine, Washington. I should point out that we have a paper that's coming out today by some of the people who are on the committee who have worked long and hard on it.

I would like to share my personal view because there are many cases where the RFID technology has provided tremendous benefits from its implementations of it even for the use with individuals in the private sector who have a number of examples such as in specialty hospitals and other venues where there is just tremendous cost and benefits to the individuals.

What we have tended to find, though, is that there are not huge benefits where you have instances where a contact card works just as well as an RFID tag so that there's no need for use of a radio.

I continue to be confused and I wonder why that's not the deployment that you're doing and not just to putting a contact card there so you wouldn't have to have something that has to be carried by a reader.

MR. WAGNER: We pre-ran the debate internally as to that exact question which is What is the right technology to use? Will a close contact chip work better in addressing a lot of the privacy concerns?

There is a healthy debate to be made in either direction. We looked at it from what's the easiest and the most reliable way to read it from a traveler perspective.

A car pulls up and there are four or five people in that car, from the time factor of putting each card up against the reader you're going to add a significant amount time to that inspection process.

You have seen the border and you seen the long lines of cars so if we take that amount of time with each type of vehicle it just has an extremely excessive wait time.

So we looked at it really from the ability to have multiple reads of that long range vicinity, RFID, the least amount of action that is necessary by the traveler who just really needs to hold it up rather than actually placing it up against the reader where an officer takes the card and place it up against the reader.

COMMITTEE MEMBER HOFFMAN: I have a follow up to that. That was the same response we got in Blaine and I did not understand it then and I still don't understand it now.

I am assuming that the line still has to stop at the point where the people are getting to the actual person whether or not the RFID tech had read it earlier on. I am perplexed to find out why is just reaching out a window to swipe a card against a reader is going to equate to long tremendous wait times in the line.

Has there been a study that's been written on that that could be provided so we can understand this?

MR. WAGNER: No, we don't have any studies that were done on it.

It's just our past experience with people having to reach out of a window with different size of vehicles with different size in travelers.

It is not uncommon to see a car with ten people in it, even four or five people in a vehicle and doing them one at a time where they are reaching out of a window, who are

dropping their documents, then having to stop to pick them up, these are all things that will lead to excessive wait times.

One traveler who takes their time to fish for their card to get it out, then putting it up against a reader, dropping it, that will snowball against that whole line of cars waiting to come in.

We felt the long range type technology will mitigate a lot of those passenger behavior-type concerns and the fact that we are only transmitting that file number, so we are reducing - not eliminating - but we are reducing and mitigating the privacy risk of what could be stolen from that signal.

We are also looking at things such as issuing the card in a protective sleeve when it is not being used and then people cannot read it.

These cards are difficult to read even with a long range type reader. We found that people do have to hold it up at a certain angle to be read. For people who keep it up against their body, those that have it in their pocket we are not finding that we are able to read them.

We think with all of these factors, in summation, this will be the right way to do it by providing some type of solution that will be of benefit.

CHAIRMAN BEALES: Charles Palmer.

COMMITTEE MEMBER PALMER: Thank you. Let me verify this first. You said at no time has there been an efficiency or an accuracy study that was done for this to show that it really makes a difference?

MR. WAGNER: We did some internal modeling which is based upon what we calculated the times would be to actually have someone hold a card up and read them versus just everyone holding their card up in front of them and reading them all at the same time.

COMMITTEE MEMBER PALMER: A follow up question is, you touched on it briefly, some vehicles have more people in them than others particularly tour buses and the tough scenario, at least to my mind, is when you have a bus of 40 people and you have 39 RFIDs read, you still have the board the bus. Is that the process? What do you do?

MR. WAGNER: We still have to board the bus and we still have to confirm the identify of each card holder.

Reading the card itself does not do that. It just says the card was read, but we still have to confirm that this is the person. But now we have just read 39 out of the 40 people and we have queried against a watch list of 39 out of 40 people.

That has just made our job that much easier so that we do not have to do it one at a time and query each one because we already know 39 out of those 40 people may or have something that may be of interest to us.

COMMITTEE MEMBER PALMER: It just seems to me that if the inhabitants of the bus, all of whom are traveling from another country who may have familiar faces and attire, they might all be somewhat hard to differentiate especially when one or two of them are missing their ID cards. Is there training for something in place to expedite that?

MR. WAGNER: We can process buses in different ways. At a lot of locations the bus parks and everyone gets off when they enter the United States, they are the pedestrian-type traveler, so they walk up to an officer who is in a booth. This is more like the airport-type situation where we read or run your documents at that point.

There are other places where we just go out to a parking lot where everyone gets off the bus and we visually confirm each one of the documents.

COMMITTEE MEMBER PALMER: How much, if at all, does a correct match in the database --

MR. WAGNER: Sorry, I didn't catch --

COMMITTEE MEMBER PALMER: How much, if at all, does a correct match in the DB, the database, modify the accuracy of the search parameters for that person or that of his or her vehicle?

MR. WAGNER: A lot. If a person is a match to a database record, then those are people who we are absolutely going to check and depending on database record says it may be a quick cursory-type search or it may be something where we do 100 percent on them and bring in everything we have and call in the FBI to interview them. It depends on what that record is going to say.

COMMITTEE MEMBER PALMER: So a good guy is someone who is in the database where they say this person is trusted.

MR. WAGNER: That allows us to expedite the entire process. As we have heard there are several things we do in that inspection process. One is to confirm the identity. One is to confirm their admissibility into the United States which are our Immigration requirements.

There is also the Customs and the Agricultural requirements which is, What are they bringing in with them? What do they intend to do when they get here? What were their intentions when they were overseas?

So what this does is that it allows us to expedite a big portion of that entire inspection that we can quickly confirm their identity and/or their admissibility into the

United States and then focus on, What are you bringing in with you today? And that allows us to expedite the overall process because we have done a lot of that adjudication work up front.

COMMITTEE MEMBER PALMER: So if you find something suspect where they might lose their trusted capacity is that the only way you can lose your trusted capacity?

MR. WAGNER: The trusted traveler programs because they are voluntary we do take a very strict approach as far as who gets in. They are zero tolerance for any type of past criminal behavior, if you're under investigation, or if you're on a watch list, then you cannot be in one of these programs. This is different than the Fast card.

This is a voluntary-type program. This is a convenience-type program. This is a benefit. So, yes, if we do uncover any type of violation usually you will be removed from that program.

CHAIRMAN BEALES: Joe Alhadoff.

COMMITTEE MEMBER ALHADEFF: Thank you. As we are looking to develop new programs and rolling out their cards one, there seems to be a gap and perhaps it's addressed by the fact that this is both a Canadian and a United States operation is we seem to get good information on people who are coming in and little to no information on the people who are going out.

Will this facilitate getting some of that information because you can exchange the in-coming information from the Canadian border side or is that still a gap?

MR. WAGNER: For the most part that is still a gap because the people who we are going to issue Fast cards to are United States citizens so we're not tracking their period of stay in the U.S. obviously.

While we do have the authority to check them leaving the United States and what it is they are bringing we are not tracking that type of information for citizens, so that the RFID in this case really wouldn't help us with that.

CHAIRMAN BEALES: Jim Harper.

COMMITTEE MEMBER HARPER: I was just interested in the data retention practices under Century, Nexus and Fast and how long you anticipate data might be maintained under the passport card?

MR. CASTELLI: The data retention, and I'm trying to remember what was said for global, was it seven years?

Seven years?

It's after they get rid of the card, isn't it? Obviously we continue to retain the data for as long as the card was active, but once the card ceases to be active where either we

removed it or the person carrying it had turned it in, then the data would be retained for a period of seven years following that.

Some times people change what it is they're doing, they no longer want to keep their card, but then they change back and then they want to get their card again, then they have to renew the application, this is just to keep that information available so we can deal with what. So that's a seven year period for that.

What was the other point you had?

COMMITTEE MEMBER HARPER: What is anticipated for the passport card?

MR. CASTELLI: I think for the passport card it will probably ... Well, yes, to the extent that it is being issued by the Department of State I would defer to that in that respect.

COMMITTEE MEMBER HARPER: Let me ask a clarifying question. The PIA for WHTI, is it anticipated that you may store the information in a database and retained for 40 years, the TECS database where operationally necessary, so where does the seven years come from?

MR. WAGNER: We have a separate database for the Trusted Traveler programs to manage your enrollment in your status in the program. When you cross the border and actually use that, it creates a record in this other system.

MR. CASTELLI: For border crossing there is a database that's within the Treasury Enforcement Communications System where we collect all border crossing incident information just as a way to separately describe it.

We are in the process of putting together a system of records to pull it out of TECS to give it more transparency in that respect.

I don't know if they're inclined to leave it at that simply because we're not all that inventive either and I think if we use border crossing information it is going to be what kind of information is collected.

But, yes, right now the current TECS system of records notice was published most recently on October 18, 2001, that indicates that record retention will be as long as is operationally necessary. It also indicates there is a periodic review and when it is deemed no longer relevant they are removed, and obviously, we can only imagine what that really means, but basically stuff sticks around.

We are in the process of trying to put an outside limit in on that and that is where the 40-year period first comes from and there are numerous discussions as to how that works.

CHAIRMAN BEALES: Larry Ponemon.

COMMITTEE MEMBER PONEMON: I really appreciate it, so thank you for being here. I would like to ask a basic question which may be due to my lack of understanding of the program, so I apologize in advance.

It seems to me that Phase I is a United States/Canada border and then Phase II is the United States/Mexico. Now a two-part question.

Does it include the US and Mexico border? Yes, if you would look at this as the air travel phase and then land and sea. So Canada and the U.S. will be done by air, but then the land would simultaneously with Mexico.

So my question is: How do you protect or prevent enrollment here? In other words, say you're a drug smuggler, or a terrorist, just a bad guy, wouldn't it be a really good idea to get a credential like this and supposing you have a criminal history which is not in the United States, but in Mexico, how does the vetting process work that gives you a level of confidence that this person is worthy of this card.

Because the way I see it, it ultimately would be the easy pass where you're driving through the border and you're dauntless, and yes, you get through and you just happen to be a seriously deranged criminal, so at the end of the day how do you reduce that risk?

MR. WAGNER: That's an excellent question and thank you for bringing that up. That is our greatest fear that these types of people do infiltrate these programs and do we get people who do that.

We just caught an 80-year-old man on the Nexus program with 100 pounds of marijuana that was found in the trunk of his car. We had a 70-year-old grandmother coming back from bingo with 15 or 20 pounds of marijuana that was found in a speaker box in her car who was coming out of Canada.

It happens.

That is why we still have you stop because we still have to figure out what you're bringing in that day which allows us to expedite it, but it is not a free pass.

What we do with the data is we can fill out the application. We run it through all the databases that we routinely access, and that is TECS, where TECS has all of watch list information, your previous Customs violations, your immigration violations, there are 40 something different agencies that contribute information into the TECS database, the DEA, the ATF, there are all sorts and types of enforcement records.

We also run your fingerprints to run your criminal history through the FBI. We also do the interview with the person where we look for your behavioral response to certain-type questions.

It's really a judgment we're making about you because you are known to the United States as a low-risk trusted traveler.

The benefit of Nexus is the Canadian government does the same thing when they access their criminal databases so you have to have approval by both countries.

We don't exchange that derogatory information routinely with Canada. We just exchange, Yes, you're approved, or it's, No, you're not approved.

Canada has a similar strict type of approach with zero tolerance so they will just tell us, this person is not approved, and they do not necessarily tell us why.

I say that that's an excellent question you brought up because we do not have that capability in Mexico because the Mexican government just does not have that type of database where they can run travelers against. So it's a huge risk for the program because we just don't know. It just doesn't exist. We don't have any visibility into somebody's life in Mexico.

This is a risk we take and the option is to not allow anybody who lives in Mexico into the program which may negate the true benefits of what we're doing with the program, but it is a huge risk and we do from time to time talk with the Mexican government about other ways to address this problem.

Is there anything we can do?

COMMITTEE MEMBER PONEMON: Are there commercial databases that are potentially available in Mexico that you're aware of?

MR. WAGNER: Not that we're aware of. We don't access any commercial databases for admissibility into this program. It's pretty much just all government databases. I mean if there were we would let you know.

COMMITTEE MEMBER PONEMON: Thank you very much.

CHAIRMAN BEALES: Lisa Sotto.

VICE CHAIR SOTTO: Thank you. I have a question on ATS. I will confess to having read the PIA only briefly and then skimmed it so I may have missed plenty that was in there. I would love some additional clarification if you would help with that.

There are two parts that deserve some clarification. The first is this 40 year retention period. It seems to me what ATS is, it's essentially a conglomeration of lots of different data that has already been maintained in different databases and that the really only new aspect and maybe this is not new, so tell me if it is or it isn't, is the scoring piece.

With respect to retention what I think I read is that each of the individual databases that feed into the ATS system retain the same retention period that they would otherwise retain outside the system.

The question boils down to: Is there any PII, person identifiable information - I don't care about meta data - but PII that is retained actually longer than it would have been otherwise that falls outside of another retention period that would otherwise attach. I will ask my second question after you answer that one.

MR. CASTELLI: I think the answer is no. What ATS is going to do, when data is run against the various databases and we are identifying information, when that data is run against the various databases, the various rules that are placed in there by Customs officers, so when we say fire there is a logical query that is run with a series of answers that come back such as some or a little or a lot, or none, that kind of thing, and from that there's a value or a weight is assigned so that when you run a number of these queries you then get a total assessment.

When we say that it retains the period of the underlying system, for instance, if it queries because a person has been identified as a trusted traveler, GES, to find out when that crossing is made, what information is there, the information that underlies the rules that fire will not continue to exist longer than what remains in GES.

All that ATS has from any of these databases is essentially an image. We described it as a real-time or a near real-time and near real-time means that the updates do not occur instantaneously, but there is a time lag of, say, 15 minutes.

The intent there was to say if the underlying data, where the information is actually being maintained by the agency, it no longer exists and it is no longer relevant to keep information relating to the rules that were used for the query or the results of the query because to the analyst who wants to follow up on that information there is no longer a means to do that.

That's why we say no longer than that. That's why, if I am understanding your question, I would say that the answer is no. That there will no be personal information, or PII, that is retained longer than the resident system simply because the information that ATS really has is just what I will call a point to or is a linkage back to that system where it is being maintained in the database.

VICE CHAIR SOTTO: Thank you. That is very helpful. My second question hinges off of this a little bit.

When we talk about the scoring it seems a little bit subjective to me, more subjective than other objective factors like is somebody on the watch list or not.

How does one go about seeking redress when you're dealing with this slightly more subjective system?

MR. CASTELLI: Redress obviously is a problem in the sense that when you look at ATS information, it's going to have essentially for each travel incident there is a score of,

let's say, determined for that incident for that person and there is a list of rules, that assessment itself, that total value of that score is not something that, frankly, we didn't obtain it from the individual so it's not going to be possible for them to say it should have been 200 instead of 180 or instead of 300.

There is no real redress mechanism for what that value is. The redress mechanism really is, was the information in those other databases accurate and when those rules fired against it. Well, are you on a watch list? And when the rules went into TECS, and said, here's the name of the person. "Here's the birth date information that we have, is there a match to a record in TECS coming from a watch list?"

If the answer that comes back is yes the point value associated with that, and the point values are standardized for all travelers, so whatever the associated point value would be using point value to go along with the scoring analogy, whatever that would be, obviously it is very high, Because if you're on the watch list, we're going to look at you.

In that context if you want redress, then the true redress is: Why am I on the watch list?

VICE CHAIR SOTTO: It just seems for the individual to try to figure out, what happened? Why am I being restricted in my activities? How do I determine which list I need to address? Who do I go to for which list to fix this?

MR. CASTELLI: Partly that's why in part of the privacy impact assessment we included what we refer to as the IBIS fact sheet, the Interagency Board Intersection System.

For many years TECS has been co designated as both the Treasury Enforcement Communications System, and the Interagency Border Inspection System, and the reason for that is it was recognized when people are referred to secondary, and I am speaking principally in a CBP context, typically what happens is we obtain the information from them coming to us in terms of their name, or their birth date, or it was something that came off their passport which will conclude that, so we ran them through TECS on primary which means we have run them against the various databases to see if there was a positive match to that name and to that birth date.

If that came back they would typically refer to what we refer to as secondary.

So when they went to secondary we attempted to clarify, at that point, for instance, is this the right Ted Kennedy we're looking at? Well, you don't look like a senior senator from Massachusetts.

It really depends on whether or not we have the right person because at that point all you know is you have a name match.

The reason why we included the IBIS fact sheet is this. Whether or not ATS ever identifies someone as being someone who we might want to inspect more closely, the main reason for why that happens is because of the interaction in the secondary and it is because the information most likely is resident in TECS.

It is at that moment when the issue comes up, when the person is saying, I am being stopped and why is that? We are giving them, and we always have over probably the last 20 years on this IBIS fact sheet, say, here's how you need to contact us about clarifying this information if it is not correct.

We have other ways of addressing misidentifications as well and I guess this was within the last nine months we started a program called Primary Lookout Override, which is what we refer to as secretary, we can conclusively determine because we have the record here in front of us that says it's a positive and we you, the personal information that is in front of us and it clearly says it is not a positive match.

If you're a Ted Kennedy, remember, there are lots of Ted Kennedy's out there. One is a terrorist. Another is a senior senator from Massachusetts. The rest is just neither, and the neither, I think maybe as to some of them they would not want to be associated with the senator, some would prefer to be one, but certainly not the other.

The point of PLOR, which is the acronym for Primary Lookout OverRide, the point of that is to basically code the record that says, "Here's a match, with typically a passport number from the person who is right there and then and says, but not to this passport, not to this individual".

So the next time when that person comes through primary the record indicates they are not a match so tat we do not have that secondary incident anymore.

That, we think, is a very effective way of recording on the spot redress that has an actual immediate positive impact for that person.

MR. WAGNER: Just to add on that. We would like this approach because the traveler has to do nothing because we do it all automatically once we confirm that you are not the person we are looking for.

We implemented this last February and to date we have avoided inspections of over 13,000 times since February 2006. So we think it's pretty successful.

We have been operating now in all of our environments, which is now sort of an ingrained process now on how we do business. It's having a lot of positives for us too because we really do not want to stop the same people over and over again. It's not worth our time either. Now, we have the ability because the system does do that work for us, so that in 13,000 instances we have not wasted our time nor have we the passenger's time.

CHAIRMAN BEALES: I just have one brief follow up. You mentioned that the matches against the various databases are assigned weights. Could you say a little bit about what is the basis for the weights in determining the overall score?

MR. CASTELLI: When you say the basis for the weights, you mean who has decided what gets what number?

CHAIRMAN BEALES: Yes, exactly, you have a got number that most of the time or all the time where it comes out of a particular comparison, that will get a certain weight relative to other comparisons, where does that come from?

MR. CASTELLI: It comes from the National Targeting Center. I have a complete ignorance of how the NTC came up with the rule sets and how they assigned those weights, but I will take that back and try to get some information for you.

CHAIRMAN BEALES: Thank you.

MR. WAGNER: The rules are based on our historical experience of what we would consider patterns or information that will interest us when looking at that person, and it is also based on current intelligence on what might be something that we would look closer at. What it does is, you described it perfectly before, it tees up this information for us of data that has already been collected and it allows us then to individually look deeper into each one of these situations.

CHAIRMAN BEALES: This is where I am confused. Is it just a comparison of a set of rules that are based on your experience which is, I guess, the way I have understood the system, or does it go a step beyond that and combine the results of different rules into a single assessment? Does it tell me that there are these three possible questions? Does the answer that comes back, is it these three possible issues about this person, or is the answer that comes back, this person is an F?

MR. WAGNER: It's actually both and the one we focus on, really, is the first. You have these high-risk travel elements that are resident with this traveler. It is not so much the summation where we're after a 90, or 100, or whatever it is, it is more where there are some high-risk indicators here and we want to look at this person a little closer.

CHAIRMAN BEALES: Thank you. Ana Anton.

COMMITTEE MEMBER ANTON: Just as a follow up, another ATS question. What, if any, relationship exists between a no fly list, and a selectee list and the ATS-P?

MR. WAGNER: The no fly list and the watch list that information is programmed into our database TECS. ATS uses that as one of the sources of information, so it will bring it in and would highlight the fact that the person was a match.

COMMITTEE MEMBER ANTON: Do you envision ATS-P replacing the no fly list?

MR. WAGNER: No, all what ATS does is to compile the data from the different sources for us in an automated fashion so we do not have to go back.

Instead of manually running your name through TECS like we used to where we get a fax from the airline indicating who is on board, and put that through the computer running it through a different system. By the way this is only with international travelers we're talking about now. This is only for international travel.

What it does is, it just compiles this data from the different sources. It doesn't actually replace that or make it. ATS is not the real watch list and it doesn't maintain that.

MR. CASTELLI: If I may add this one other thought, and I do apologize to my colleagues from TSA who are here, but as I understand the no fly list and the selectee list are involved, they are developed from information that TSA has which partly includes the watch list.

ATS-P basically is what is in the passenger's name record and when it queries TECS, it also queries that same watch list. It doesn't actually ever query the no fly or the selectee list because that's something that is derived by TSA from the watch list and from their sources or at least that is my understanding.

Whereas, with ATS-P, it would be something that we would get from the airlines and then compare directly with TECS which would include that watch list.

It's true. They are both coming from one source of information which is shared in common between the three, but there may be other sources of information that are different.

COMMITTEE MEMBER ANTON: Say I'm a screener at the LaGuardia Airport on a flight from London, which list do I use?

MR. CASTELLI: You are a TSA screener, so you will be using the no fly and the selectee list. You're not going to get a boarding pass if ATS-P says you're not supposed to get one.

Sorry, actually, it would be AVIS that would say that which is part of the TECS system.

You're not really going to come into an issue of basically not knowing which list to use. In fact, actually, if you're a screener, I don't even think even the screeners actually use the no fly and the selectee list because that would include the airlines that use them directly, so screeners basically will resort to their own list.

COMMITTEE MEMBER ANTON: If you could indulge me with one final question. If there's a risk scoring, so to speak, for each person in the system it would seem that that should be fed into whether somebody gets on the selectee list or not.

I feel like there's a missing link there somewhere and I am just trying to understand that, and if there isn't, then why have the score and what is it used for and by whom?

MR. WAGNER: We could use the results of an inspection of a person which could be based on ATS to nominate someone for inclusion on a watch list so to speak.

TSA controls the watch lists. There is a process where we can nominate people for it, but we do not routinely give feedback just because we inspected someone based on our analysis of their different records we have. We do not automatically feed that back into a list. The possibility is there that we could uncover something, so we could nominate them.

CHAIRMAN BEALES: Let me try to clarify this a little and then maybe ask of you to confirm that my understanding is right.

As I understand it ATS-P is about who is going to be pulled aside for secondary screening coming into the country. It has a much broader set of purposes, and legitimate purposes, such as drug enforcement, for example, that have nothing to do with the no fly or the selectee lists.

On the outgoing scenario, if you can get on the plane, you will be looking at the selectee list or the no fly list to figure that out.

If you're coming into the country, then they're looking an ATS-P to figure out whether there are risk factors that would lead to secondary searching.

MR. WAGNER: Yes! Very well put!

CHAIRMAN BEALES: I got it! Thank you. John Sabo.

COMMITTEE MEMBER SABO: I would like to go back to WHTI. Maybe I missed it. I have scanned it, but I have not had a chance to read it in detail, but the only reference to the chip, or to the mechanism to identify the individual is in Section 2.3, where it says: "The information will be collected by running a machine readable ... passport scanner reader or through the use of other technology of the RFID chip."

Is that the only reference in that PIA reference to the new system of records that are created BCIS which is the information system, so I have two questions and the first subset of questions is, is that correct, that that's the only reference to the identity question, and (b), the reference to BCIS the final new SORN created, does that BCIS/SORN include the chip-based token or are we talking about different PIAs?

MR. WAGNER: We are talking about different PIAs. When this one was written I don't know that we were ready to talk about the different RFID technologies.

This PIA, I believe, was written when we were still moving forward with an air and sea rule. What we are going to be doing is we have another one more for land and sea and it will be a lot more comprehensive and it will include that information.

COMMITTEE MEMBER SABO: Thank you because it wasn't clear what was encompassed. The second follow up is: Would you be willing to share with the committee your risk analysis?

One of our framework components that was issued in March with the privacy office was a recommendation that evaluate the use of technology and one of the areas we need to look at is efficacy, that is, what is the value of this and risk management.

There was your reference to the fact and again, I hope I am not inflating these, but one of your considerations is the physical safety for your inspectors. You talked about a 20 to 30 foot distance as you referenced this physical safety zone.

From a risk perspective, it is not clear how an RFID tag, per se, addresses that issue, but that probably goes with the risk analysis, so I think we need to see what that analysis is because when you indicate that that's a factor, then that would impact the overall design, not entirely, just the RFID component of the design is what I am saying.

The reason I brought that up is because when you mentioned the Nexus traveler, the 80-year-old gentleman who had 100 pounds of marijuana that was in his trunk he was clearly inspected and that obviously took place not robotically by an inspection.

When you're laying out the rationales for using technology and then that rationale is perhaps contradicted by another rationale when you do an inspection you have to take look at the overall inspection, would you be willing to share that with the committee?

MR. WAGNER: I am sure there is something we could share with you on that. As I mentioned before, there are different pieces of that inspection process, the RFID technology addresses one piece of it, it helps us to break up the information to confirm somebody's identify and their admissibility into the United States.

It also helps our position to run that information against the watch list. It does very little to say what that person actually has with them or what their intentions are going to be unless we had a record where a person would like know that in advance. It helps us with part of the process. It certainly does not do the whole thing and it is not the "be all end all."

Between the close range and the long range, what we have looked at really are the entire circumstances and what would give us in the perfect laboratory setting, if we could get travelers to all be compliant to properly place the card up against the reader while they're waiting in line, if we would know with confidence that every person would reliably do that, then we would have picked out that technology.

It is human nature with human behaviors, those differences where logically you have different sizes of vehicles and different sizes of people, because, for instance, just observe a drive-through when you are at McDonald's you can see how some reach down and try to speak into the speaker, things like that will lead to delays having with it the cascading effect on the rest of the traffic.

We're looking for a technology in how do we mitigate that concern that will give us a more reliable-type convenient approach for the passenger themselves.

CHAIRMAN BEALES: John, I want to thank you and Larry very much for being with us today.

We really do appreciate the information that you have given us along with your being forthcoming and answering our wide variety of questions.

We need to adjust our agenda at this point and move to our hearing from Jennifer Stoddart who is the Privacy Commissioner of Canada.

We will hear from Jennifer and then after Jennifer we will break for lunch. We are doing this in order to accommodate her travel schedule because she has already spent a tremendous amount of time with us.

Jennifer Stoddart was appointed Canada's privacy commissioner by the Governor-in-Council effective December 1, 2003, on unanimous resolution adopted by both the House of Commons and the Senate for a seven-year term. Since her arrival she has led the office's institutional renewal and she has also reoriented it towards a multidisciplinary approach to preventing privacy breaches in the public and private sectors and the protecting and promoting the privacy rights of Canadians. She was previously president of an organization responsible for both access to information and the protection of personal information in Quebec. She has held several senior positions in public administration for both the Governments of Quebec and Canada including the Canadian and Quebec Human Rights Commission. We really appreciate the time you have spent with us and we really look forward to hearing from you today.

Thank you very much for being here.

MS. STODDART: Thank you very much, Mr. Chairman and members of committee, Mr. Teufel, and his staff.

I am very honored to be invited down to have had a chance yesterday to share in the work of this very prestigious and very knowledgeable committee.

I just met Hugo Teufel less than two months ago. He phoned me a bit afterwards when he was still suffering from a really bad cold, and he said, "I must come up to see you and some other people in Ottawa."

I looked outside and it was about 45 degrees, and I said to him, "Hugo, I don't think you should travel in the state you're in. We love coming down south to Washington any time after November."

Lo and behold three weeks later it got even better and he invited me to Miami.

Spending the winter in Florida is somewhat of a Canadian dream. I am not the only member of my family who will be living out this Canadian dream, however briefly it will be, as my son will be down here for a week.

He is in our engineering reserves in the Canadian Armed Forces and he will be training at one of your camps in Northern Florida. I gather the real attraction is that after these four days of training he gets to go to the beach for two days.

I prepared a formal presentation and I will just highlight it, but I will remind you that there is an "entree en matiere" in a New York Times story about the competition that ran for the world's most boring headlines and one of the winning entries was "Interesting Canadian Development."

Nevertheless, I will forge ahead and tell you about privacy developments in Canada knowing that we're often off your radar screen.

The contrary is not true, of course, for all the reasons that we both know. We are particularly following your recent move to tighten requirements for entry into the United States extending to Canadians.

I was exchanging with the chairperson on this when we used to be able to just drive across the border with a wink and a nod, and now, as Secretary Chertoff has said, for air travel Canadians will have to have passports.

That is not going to be much of a problem because a lot of Canadians do have passports, but the commercial and economic effects as you move to more stringent requirements on land transport at all the numerous border crossing points, are going to be quite significant as we have a huge interborder trade with a lot of American tourists, and to the extent that they find reciprocal requirements to come into Canada, even where we have no requirements they still have to get back to where they came from. So we have very great concerns about our border economy.

The Canadian approach to privacy is enshrined in two acts. One is our Privacy Act is more or less a version of your own Privacy Act that was inspired by your early forays into privacy.

It sets up my office. It gives me roles and powers. I am a kind of multipowered ombudsperson. I settle cases and usually I will investigate and settle cases by consensus and in some circumstances take them on to Federal Court.

This was then complemented by a new law which was developed in response to the European directive that you all know of 1994, and then Quebec first adopted its own legislation, and in 2000, the federal government did it, then several other provinces did.

This basically covers the federally regulated sector and the commercial sector in Canada except where the provinces come up to the same standards.

It may be slightly difficult, but believe me in trying to figure out the privacy laws in 50 states, yes, we have our own challenges.

How did we react to the security threats after 9/11 and what are some of the privacy implications that we share with the Privacy Office of the Department of Homeland Security.

Let me just mention that we passed the Antiterrorism Act which is in contrast to the debate that's going on now about the extent of presidential powers in a time of war and how far that could lead. Recently in the past six months two sections of this law were struck down as being unconstitutional by the lower courts, one, because it was found that it would lead to racial profiling, so we will see how this goes through the courts.

Another act, which is our antiterrorism act called the Public Safety Act of 2002, although it was finally passed in 2004, will be of interest to some of you because I think almost they are all of the private sector except some professors which made private companies for all intent and purposes agents of the state. They were then authorized to collect information about persons of suspicion and to seek out information.

So if you were to roll up to a travel agent, who is under federal jurisdiction, and the travel agent thinks you're a bit funny, the travel agent then can phone in that information to one of our law enforcement agencies.

We basically strengthened our money-laundering legislation and that's going to be strengthened once again and next week I will appear in parliament, in our Senate, to talk again about strengthening provisions for our money laundering agency called Fin-Track.

The concerns about Fin-Track and the strengthening of the money laundering provisions in Canada are not related to another debating point that's going on now in privacy circles ... the Swift Affair.

The European Union has condemned the finding and my office is investigating as are the offices of the Australian and the New Zealand privacy commissioners.

Another current issue that we share with you is the debate about the national identity card and I gather that your language for this is Real ID.

All privacy commissioners in Canada are drastically unwaveringly critical of any attempts to introduce national identity cards in Canada.

We are concerned about the right to anonymity, we are concerned about possible denial of service, automatic inclusion on watch lists being used as an internal passport as you move through jurisdictions, and increasing profiling of ordinary Canadians, that is, the profiling on non-terrorists, non-security ways just because it is handy.

So far there has been no measured attempt to introduce a national ID card and it's interesting to note that Canada and the United States who share many cultural traits are together in their public disapproval.

Let me quote from a recent study that was done at Queens University in Ontario on international attitudes to surveillance.

The question was: "Should everyone have an ID card that they carry at all times?"

In Canada, a small minority said, yes, 53 percent. In the United States, which was done in the early spring of this year, you said 44 percent. So only 44 percent. So not a majority for ID cards.

Some of our European friends, in France 78 percent thought you should carry an ID card. In Spain, 68 percent and in Hungary, this is amazing given their communistic experience, it is 93 percent.

The question is: Do these populations really understand all the privacy implications and when can they not think they are less educated about this than we are or are there fairly significant cultural differences in this approach to privacy.

I think that's one example of cultural differences let alone the cultural differences between us for example and the Asian nations which yet another challenge. The topic of airline security and border security is clearly high on your agenda so I will just speak generally about our no fly list called euphemistically the Passenger Protect Program.

It's just being introduced, the Canadian no fly list and I understand that we comply with your no fly list when we fly from Canadian airports into the United States. It is being criticized because it is against both our Charter and our Bill of Rights, and of course, the freedom of movement that is guaranteed by the United Nations Declaration of Human Rights that both our countries signed.

We are concerned that the threshold is being just a threat to aviation security and on this we are concerned that it could be something as trifling as being rowdy at a ticket counter, although I must say that the Department of Transport has done a PIA.

We asked them 24 questions publicly and they published the answers to the web site. We have not taken a position on their answers, but Canadians are very, very mistrustful of a no watch list because take your Senator Kennedy's example has stuck in many Canadian minds being the problem of false positives that many of you who are technology specialists understand far better than I do.

Even if being told by the Department of Transportation officials that it is going to be a very small list of about 1,000 names we are told, so that the physical chances of your turning up on this list are very slim.

E-Passport. We are monitoring this but we are subject, of course, to the same ICAO standards as you are.

So far the Passport Office in Canada has been a bit of a black hole. We cannot get any information out of them despite the recent requests made. I think they are watching and waiting probably to see (a) what other countries are doing, and (b), what probably what it is mostly: What is the reliable technology?

We have followed with great interest and I imagine the Passport Office follows it even more interest the debates about the ARFIS, the State Department's withdrawal of a plan for initial planning for ARFIS and passports.

We read about what happened in Denmark with their experienced in having ARFIS being read, so probably we're waiting to see what other countries experiment with and when we come up with a safe solution we will probably follow it, but that's not the official position of the Passport Office.

The single most significant American act and piece of legislation that affects the Canadian psyche is, of course, your Patriot Act that has taken on a symbolic life of its own, not only in Canada, but of course in Europe with repercussions which has caused great anxiety in the Canadian public not only because of what it purports to do, but because of the fact that even more than in Europe our personal information flows south of the border.

This is because of the high integration of our two economies and there are some of you who know these figures far better than I do.

There's the fact that many Canadians companies are in fact subsidiaries of American companies because we exchange populations, skill labor, and so on, and American attend Canadian universities and vice versa.

The powers of the Patriot Act has caused anxiety in Canadians and then there is the extraterritorial reach of the Patriot Act, it causes anxiety, that is, where you have a Canadian company that's owned by an American company can be ordered by the FISA Court to give up information, let's say, on an employee who is in Canada, so the legal theory runs and I don't have been definitively discarded, and the company cannot speak on pain of, I don't know what terrible sanctions, that the other company has received an order from the FISA Court.

The good news from the Privacy Commissioner's point of you about this public concern is that it has raised the level of privacy issues and it has raised public knowledge

about information issues about information that's been thrown across the globe in a way it wouldn't if we had not had the Patriot Act.

You may have followed the responses in Canada. They range from the Government of British Columbia passing a law saying that personal information given to the public sector in British Columbia, for example health information, and our health services are run by the government, cannot be exported.

This was passed with a great amount of public debate. Other provinces have taken variations of this position. Quebec has really changed its legislation to say that you cannot export personal information unless you're basically sure that it will receive the same treatment as in Quebec, so this suggests that you can, in fact, tie the receiver of the data contractually to the standards of the sender.

Our Canadian Treasury Board has set down guidelines on which we worked with the Treasury Board in terms of how to deal with data of personal information and outsourcing which is one of the things that we had hoped would be put into a new privacy act ... if we can get it reformed.

In interpreting our commercial sector legislation, PIPEDA, this is what we will be using in the eventual swift conclusion we have used something called the accountability principle.

This is the contrary approach to the Europeans. They Europeans say that we cannot export our data unless the place it is going to has the same standard as us.

We say, "You can export the data, but you have to make sure, it is your responsibility that it is enforceable in Canada to make sure that that data is treated according to Canadian standards abroad."

Moving on to a few border issues. In 2001, our governments just after 9/11 signed the Smart Border Agreement to strengthen our shared borders and to exchange intelligence.

We created something called IBETs which is Integrated Board Enforcement Teams and INSETs is Integrated National Security Enforcement Teams, to make us both more efficient about possible negative activities or people crossing our mutual borders.

My office has done a review of this in 2003 and has found some information sharing lacunae that are published in our 2003 annual report.

The last issue I want to share with you is our recent audit of the Canadian Border Services Agency whose head has just met with Hugo we made quite a few recommendations.

We were concerned, and the CBSA has been doing overall a pretty good job, but there were ways of tightening up the information sharing practices and we were particularly concerned as a matter of principle that the CBSA could not report on how much or how often it shared personal information with the United States.

We are just looking at how Canada and the United States flows and not how Canada and the rest of the world flows because most of our flows are with you, so we recommended the adoption of a privacy management framework to update our MOUs with you. I think some of the MOUs date back decades ago because this has been going on forever.

There is a lot greater transparency certainly to dispel the nervousness in the Canadian public about what is happening to their data on a border situation.

I have a proposal that I hope that the Privacy Office and this committee could consider and that would be that we look at the possibility of doing privacy audits in tandem with the information that you share with us, that you collect on us and that we collect on you in a border situation.

We should try and work to mutually agree on compatible standards for personal information protection and then would do a lot to make our activities at our mutual border a lot more transparent and understandable to our citizens which would give us a big picture.

I will just conclude by reminding you of our September Conference in 2007. I have some maple syrup candies left to give you the Flavor of Canada, so remind me to pass them out at lunch. I was very happy and very honored to be asked to share our experience in trying to reform our own privacy act with you yesterday.

In closing, allow me to share this saying of one of my fellow privacy commissioners, a former Australian privacy commissioner and I believe both the Canadian and the American population share in: "Privacy is the most fragile of our freedoms and we have to work hard to protect it."

Thank you once again for inviting me, Mr. Chairman, and members of the committee.

CHAIRMAN BEALES: Thank you very much. Our first question will be from Tom Boyd.

MR. BOYD: Thank you for joining us this morning. I gather the course of your efforts to perform your privacy act there are number recommendations that are emanating from your office which I am sure involves some interaction on your part.

I am wondering if one element of those recommendations has to do with enhanced privacy enforcement, again, with what's available in this country for consumers such as privacy rights of class actions and the like. Is that part of your reform movement?

MS. STODDART: That's a very interesting question and thank you. We haven't thought that far as to private rights of action in the context of privacy rights.

We have certainly have recommended that there be increased rights of actions and damages because as you can see there is very limited right of action, but generally I think the individual should private rights of action across Canada that we don't have a developed privacy toward as people cannot go to what we would call small claims court to enforce their own privacy rights.

Probably I will federally because although we have a different model of government than you do in your role perhaps for some of our administrative agencies, I think people have to be able to enforce their rights directly and not to depend on government agencies and it is only at that time that you make the right -- Well, someone yesterday was talking about enforceability and redress.

We are short redress for privacy, so probably we will go there.

MR. BOYD: That would include class actions and the like?

MS. STODDART: Yes, and doubtless in the form of PIPEDA. I know there are some advocacy groups that are going to recommend class actions. PIPEDA is our commercial sector legislation and I would agree with that. Yes, I think it makes those who would be negligent of privacy law or take it lightly to have them sit up and pay attention a lot more.

MR. BOYD: Thank you.

CHAIRMAN BEALES: Lisa Sotto.

VICE CHAIR SOTTO: Thank you so much for joining us. It has been really our pleasure having you here. This is more of a comment and not a question.

As private sector lawyer I represent a lot of global companies many of whom are extremely concerned with the lack of uniform framework around the world through which they can understand the rules by which they would be sharing data with the government should the government come calling.

Clearly, we have seen this arise with the Patriot Act and we have seen it more recently with Swift. There is really deep concern in private industry and these are companies that are enormously responsible and they do want to be responsible and they want to comply with the law of whatever jurisdiction applies, but they do not know which law applies.

I would urge you and Hugo and all of the other government privacy leaders to come together to help private industry in that regard.

MS. STODDART: If I may make comment in response? Yes, this is a hugely important issue in spite of my office's previous reputation and that's why I think international contacts is a key especially for a commercial nationwide Canada as we live from our exports in order to develop, hopefully, universal privacy rules that are certainly consistent privacy rules with our major partners in order to facilitate exchanges.

However, we all have to work to make privacy come higher on the government's agenda because only when there's a meeting of the minds among our governments in a major way are we going to get some resolution of who laws apply because we are in a very acute situation with a conflict of laws right now and there is no court to take it to or is there no court that we all recognize to try to solve this.

It is a major diplomatic issue.

CHAIRMAN BEALES: John Sabo.

COMMITTEE MEMBER SABO: Thanks, again. There was a suggestion about a Canada audit and I wonder if you have done or would consider doing or have news about a tandem or a collaborative development of PIAs on systems that impact Canadian and U.S. citizens who like western hemisphere travel an issue?

MS. STODDART: No, I hadn't, and I would guess that that's a natural outgrowth of doing an audit. It might be easier meeting PIAs. I think PIAs are starting to have a kind of universal approach and I would be very happy to talk to this office further if that interested this office.

Clearly, and the acronym just escapes me, the Secure North American Hemisphere, the Northern American Perimeter? Yes, but I believe there is yet another long term plan which has to do with the whole continent of North America.

I understand that long term there is over five or six years this idea of working Mexico, the United States, and Canada into a common framework of securities that is something akin to the Shamus Accords in Europe and certainly in that context, and I cannot speak for Mexico, but for Canada that is going to mean that we will have to increasingly look to common standards to enter into the Northern American space and it would make sense that those of us who are concerned with privacy look to have equally forceful privacy standards in trying to reinforce each others attempts to make privacy included.

CHAIRMAN BEALES: Joe Alhadeff.

COMMITTEE MEMBER ALHADEFF: Thank you. I also join in thanking you, Jennifer, for participating in the meeting and giving us a lot of your time.

The accountability framework, which was pioneered in Canada and has found its way into APEC with a broad range of applications, so there's a lot of benefit in looking at that.

I want to pick up a little bit on Lisa's question because I know that your comments were limited mostly to the cross-border context of Canada into United States, but as we look at the lawful access issues, and these are conversations that I have had with Commissioner Lou Gellas as well, and others, we find that in almost every country there is something similar to the Patriot Act.

It may or may not have the same level of a notice prohibition, but it's very similar and in fact Canada has some aspects of the Patriot Act in its law as well and those cross-border lawful access requests predated the Patriot Act by 15 or so years at least in their current version.

We also have to be cognizant of the fact that these issues have gained a political loss as well as a functional parameter.

I guess the question would be as you go into the perimeter revisions and looking at these issues and you're looking at the RFP Act in the UK, and the other acts that are specifically relevant, is there a way you can see to help divorce what has been a political fire storm around what is a very legitimate functional issue?

MS. STODDART: Those are interesting comments and my referrals to the Patriot Act didn't mean that I'm not cognizant of the fact that every country has national security and antiterrorism legislation who have probably had their equivalent for decades and we certainly do in Canada.

I just wanted to point out the symbolism which is rightly or wrongly taken on and how politicians and privacy commissioners have to respond to this and explain to Canadians that they have their own national security legislation and so on doesn't seem to reassure them about it, and of course, the size and the importance of the United States means that it takes on life of its own.

I am not recommending major changes to PIPEDA to prohibit the outsourcing of personal information. Far, far from it. I am basically taking a minimalistic approach. My submissions on the web site, I have suggested some housekeeping issues to make it work more practically within Canada and I think the accountability principle is an appropriate way of dealing with it.

We suggested that if the government does want to tinker with PIPEDA and I would be surprised at this particular juncture that they incorporate the Canadian Treasury Board's guidelines about sensitivity of material and things like that, but they would be guidelines.

CHAIRMAN BEALES: I would just like to note that I like your statement of the accountability principle because that is certainly the position that the Federal Trade Commission has taken about data security for United States companies, that they are responsible and that it doesn't matter where the leak happens, that it was their responsibility to keep it from happening whether the leak happened at home or abroad if it was their data, that it was their responsibility.

Also I believe bank regulators have taken essentially the same position that data is protected by U.S. law and companies are responsible for that.

Are there any other questions from the members of the committee? If not, then I will declare it to be lunch time. Please be back here at 12:30 so we can resume at 12:45 for the afternoon session. I would remind you that Lane Raffray is in the back of the room so if you're interested in signing up for public comments we can accommodate you all, so if you would like to speak, please sign up. Thank you and we will see you when resume at 12:45. (Afternoon Session.) 12:45 p.m.