



Homeland Security

DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
FULL COMMITTEE MEETING
WEDNESDAY, MARCH 12, 2008
Wyndham El Paso Airport
Sandalwood/Satinwood
2027 Airway Boulevard
El Paso, Texas 79925

AFTERNOON SESSION

MR. BEALES: If I could ask the Advisory committee to come to order. Our first speaker this afternoon will be Peter Pietra who is the Director of Privacy Policy and Compliance in the Transportation Security Agency, HHS -- DHS. Peter joined TSA in 2003 and has been with us, I think, on more than one occasion before.

He is responsible for privacy matters affecting the traveling public and workers across the transportation sector and more than 50,000 TSA employees at 400 locations.

Peter started his legal career litigating insurance and intellectual property matters in Wilmington, Delaware. He is a graduate of the University of Pennsylvania at Temple University School of Law.

Peter, welcome back and we look forward to hearing from you.

MR. PIETRA: Thank you, Howard. Thank you to the committee for inviting me, and to DHS for paying my way. I provide this update on where we've been in the last year, last couple years, a year ago.

Overall, the last two years have been a busy time in the federal privacy world, partly because of the shift in paradigm from a Privacy Act area of concern, to a PII area of

concern as illustrated in all the memos that talk about PIIs, a new area to be concerned about.

There are -- having been expanding and shifting data mining definitions that require different analyses within federal agencies, and a lot of pressure to do information sharing with information sharing environments that break down what had been traditionally traditional barriers between different parts of agencies and between agencies, and that used to get resolved when a person would go in, knock on a door and say I need to see somebody's file, kind of resolved, and now that's all going to be done electronically, and it's going to be a very different, different world.

In the last year we've published 11 PIAs. Some of the more prominent ones include the Secure Flight MPRM, the TWIC Final Rule, the Commercial Driver's License Order, the Vetting Program, different Certificate Holder Vetting Programs, Boarding Pass Scanners, Full Body Imagers.

And, we've got eight or nine others that are in the works right now, and I'll talk a little bit more about some of those programs as I go on. The shift to a PII world, Privacy Act world, is significant, mostly as a training matter.

It's difficult to get people to understand that -- where you used to and still do have to think about Privacy Acts records and that was the trigger for a bunch of your obligations for certain kinds of records.

Now you have to also consider whether information that may not be part of system records but may be sensitive for other reasons has to be secured different ways. We haven't felt that a lot of the guidance at upper levels has been so broad as to make it impractical.

You get the definition of PII, which is appropriately broad, which is PII, but then you are told that you have to encrypt it. Well, you know, if your name is PII and your work e-mail is PII and then you send it, I don't know how you are supposed to encrypt that to prevent it from getting out.

So you've got to kind of have a more practical view on what is really important in the world of PII and TSA. We made an effort to narrow it down to what we call sensitive PII as things like name or some other identifier with a Social Security number, driver's license number, alien file number, medical information, financial information, your electronic funds transfers, system IT passwords, things like that that make it a little more realistic.

So that if you, quote, unquote, lose a telephone book, you are not -- you are not in a data-free situation. At the same time, build in the possibility that you may have a list of names that by itself is significant because it's a list of employees that are about to get fired

or a list of employees that have certain medical issues. That obviously would need to be protected.

So we wrote a policy. It's a page and a half. So that we have very direct guides to our users. It's the kind of thing that they can tack up in their cube and understand pretty quickly what exactly are your obligations for our data, hoping that the DHS is going to adopt it. I talked to Becky yesterday. It looks like that might actually happen.

Some of the other things we've done in terms of protecting information -- I try to look at it and tried to automate. Those protections have been using an enterprise writes management tool to try to force certain types of protections on e-mails so that every e-mail that is sent has this sort of protection automatically.

If it makes its way outside of the agency by mistake and it's encrypted, the recipient won't be able to open it. It hasn't been that successful. I haven't been able to figure out how to do it -- because there are cases where you have to send e-mails out. And forcing every employee to check a box with every single e-mail, I think, would pretty soon become a practice of people checking a box without thinking what they were doing. So that's something I'm still looking at.

And I think it's important to try to figure out ways to eliminate, as much as possible, the human factor. We looked at installing RFID in our mobile devices so that if they ever left the building we would know it, and if one went missing, we would be able to take a look at when it went. And if it was captured on video, see you walk out the door with it.

Again, as a practical idea, it may not be a great idea because the human body blocks RFID signals. There are other ways to get around it. There are some practical problems with it that may not make it a good solution, but it's things we spent some time looking at.

We did encrypt all of our mobile devices, all laptops. We're, I think, in the process of encrypting desktop computers as well to try and get a real -- a better grip on protection for our information. We have a pretty robust reporting process for U.S. CERT. We do have data readers. We stood up the -- being responsive a year ago. Unfortunately, we hadn't really gotten to use it. It was two months after we stood it up. It's unfortunate we had to do it. It's fortunate that it stood up and it worked very well.

We had it reported on a Thursday afternoon, about 4:30 in the afternoon. Before nine o'clock the next morning we had the group assembled and by the end of the day we had a plan, including how to get a notification out to the affected employees, had contacted Congressional representatives so they understood this was coming, and stood at the ready, contact center by the next day and started the process for taking advantage

of DPA to get identity theft and credit honoring service for all our employees that were affected by it.

And they also had a couple web broadcasts that our administrator spoke on to tell employees exactly what had happened and what efforts we were making. So it's unfortunate we had a breach. It's a good thing we had a team in place and were able to respond very quickly.

Last year I had mentioned that I was working on trying to build into our acquisitions process privacy in the RP stage so that people would be forced to address privacy aspects in their proposals as well as building in an evaluation phase so that when a contractor bid on a contract that involved access to PII, then they would have to address, you know, what they were going to do for privacy and data security.

That wasn't adopted as part of our acquisition process. I'm unhappy to report that I just learned that we have been required to handle a FAR process. We've been taken off of our old acquisition process. Now I need to start all over again trying to get these added on to the standard FAR process.

I don't know how long that's going to take. That's a bit of a blow. We have a pretty robust outreach effort. I meet every Monday morning with Kip and our senior executives, and I have Tony Johnson who is, of course, in my office as well. And I have established great rapport with all our different program managers.

So we've done a pretty good job, I think, in terms of making them aware that privacy is an issue for virtually all of our programs, and meet with them. We have had a variety of different outreach broadcast messages to our employees to talk about different things, including proper handling of PII, making sure that you destroy records that have PII instead of just throwing them in the trash to prevent dumpster diving.

We've had a couple broadcasts over things that weren't things that really affected TSA but were things that we were concerned about. So somebody -- and I'm not sure how this happened, but somebody realized that there was an SF-86, which is background information posted on the internet on Line Wire, which is a peer to peer file-sharing website.

I was really concerned that the source of that file was our HR department. And so we contacted the person whose information was on this Line Wire site. It turned out that her daughter used it for sharing music, and it had been pulled by Line Wire and posted from her computer, not from a TSA computer.

This is a problem that you have and here is how you fix it, and then we were able to broadcast the next day to our entire workforce saying this is something you may have on your personal computer and realize it. And we gave them lists of some of the more popular file-sharing sites so that they would understand, oh, I use CaseEye or whatever.

Look at the security sites they had for their information. A lot -- we got feedback from a few of them. This is something they hadn't been aware of and it was a great broadcast. At the same time, I have to admit that our workforce -- 90 percent of our workforce does not work with computers every day.

Our workforce are the TSOs that are at the airports. They don't use computers, and they have only limited work time to look at their computer accounts. And so I don't know how effective all of our broadcasts have been because of that kind of practical limitation. And that's something that I've got to try to address going forward to make sure the information that we do send out gets disseminated somehow.

I want to talk about some of our programs that you are aware of, Secure Flight. Again, TSA was directed by Congress to assume the existing matching process that the airlines use. And we have had -- published an MPRM last August, held a public hearing in September. Kip attended and spoke a great deal at it.

We received comments at the hearing from, I guess, about 25 different individuals and some organizations and then received another 300 or 400 or so comments to the MPRM. A big chunk of those comments were addressed as a constitutional concern that this was somehow a violation of the Fourth Amendment.

And we are currently in the process of preparing the final -- actually, it's almost done and it will be on its way through -- I can't really talk about the specifics of what we are going to be saying because it hasn't gone through yet.

I can't really say that in this forum, but some of the things that I really was concerned about hearing, getting comments from the public on were the data analysis that we're collecting, the notice that we're proposing to provide to the public.

We got comments on some of those issues. Unfortunately, the comments were all over the place. Some of them wanted -- including one person who wanted more information, something that I hadn't expected because they wanted us to get nationality, I think -- or I can't remember now, but it was an element that I hadn't been aware of.

The idea -- or the benefit, I guess, behind Secure Flight, eventually, we hope, will be a more uniform application of the rules, and that ought to eliminate -- and then a more uniform application of the cleared list, which ought to reduce down the number of people who are flagged for secondary screening or identified as possible no flies for flying.

The TWIC program is up and running. It has enrolled 150,000 workers already. There are -- they printed about 62,000 cards. Of those applicants, 2,000 received initial disqualification notices. 1,000 of those appealed or submitted waiver requests, and only 15 have gone to a final disqualification.

So the percentage of people that are receiving final disqualification appears to be very small compared to the overall population, which is a good thing. It's been a very effective, I think, redress process since we were talking about redress this morning.

The TWIC program established -- worked closely with the MTS Act, which is a Coast Guard Maritime Security Act. They had a couple different public hearings and selected comments on what the card ought to consist of, what the security features of the credential ought to be, and resolved that the PII on it, the fingerprint template, would be encrypted despite the view that -- of some that that shouldn't be encrypted.

And the process is that the worker gets to a reader, puts their finger on the reader. And they will have -- they are a contactless feature, which will be from a small distance or swipe the card. Unfortunately, we don't have the reader specifications developed yet, and that's the current effort for that program.

The idea of using a PIN to release the encryption was rejected based on the operational requirements, and on the environment which is a pretty harsh environment in the maritime area. We're still very interested in a Match-on-Card as to a potential solution to a lot of the problems with the card, but there aren't any specifications yet so I think that's going to be pretty far down the road.

Oh, and on TWIC we have -- there are 82 enrollment centers that have opened out of 89 that were announced so the enrollment establishment is pretty far along.

Whole body imaging, I talked a little bit last time I was here about the technology that we have under some pilots, and it's millimeter wave and x-ray technology. Those pilots are still ongoing. They are being expanded. It started off with Phoenix, and we did quite a bit in both the media and on our website we have a pretty thorough discussion of it.

The PIA has a pretty good discussion, I think, of providing imaging, including actual images of what is involved so you can take a look and see. When an individual comes up to one of those devices, it will also show what it is that the reader or the viewer sees when they see it so that the individual can make the decision whether they want to undergo it.

It will be voluntary in both secondary and primary. If you don't want to do it, then -- for primary, for example, then you would go through a megatometer and get the pat-down. Secondary, it is also voluntary but the option is a pat-down, and so far the public seems to be really accepting the full body imager and embracing it.

It's a 94 percent preference for the imaging and than getting a pat-down. It's the same technology, the same process that's being used in Europe. I think it's planned for use in Japan, and so it's -- I think eventually will be more widespread.

The PIA discusses some of the concerns about radiation exposure, things like that. X-rays are equivalent to about two minutes in flight at altitude so it's a very low dose. And the radio waves that the wave meters use is 100,000 times less than. So it's very, very little energy that is produced by these things.

And the principal privacy protection for these devices is one that we stuck to, and we pushed hard, and that is we do not retain any images at all. I note some of the nongovernmental organizations have expressed some skepticism of that, but we really don't retain these images. We don't retain them for enforcement purposes, if we find somebody to prosecute them. We don't retain them for training. It's just not retained, and that's something that I hope we'll continue through the operational phase. And I expect that it will.

And then the other is that the viewer of the imaging is remote from the person coming through so the people who are looking at the imaging never see the person that is actually walking through the checkpoint.

In some cases it's expected that the viewer will be in a completely different floor. Right now there are drywalls. They are in a little room. It's dry walled off. And so that kind of ensures that there is no possibility that there will be --I have some new things to talk about.

I think in many ways TSA is going to lead the rest of the world in terms of surveillance. I think one of the recognitions is that identity-based security has weaknesses.

And so one of the answers to that is to take a look at behavior-based things. Unfortunately, to figure out what behavior-based security risks have, you have to do a lot more surveillance. Some of it is, I think, what you expect on CCTV.

All the airports have CCTV. Almost none of the CCTV out there currently is TSA controlled or even TSA funded, but that's going to change over time, and establishing a protocol that is going to be appropriate for that is something that is still in the works.

I'm very happy that TSA or DHS had a CCTV workshop in November to talk about these things and got a lot of participation from both law enforcement and from the ethics groups. ACLU and CDT and some others were all participants in a workshop.

To date, for the cameras that we do have, because the images are anonymous, we haven't really had significant privacy concerns, but at some point -- I don't know if that may -- that will change, but it might.

People talk about facial recognition. I don't know if that will ever happen. I saw a great demonstration. I guess it's a website where you can send your face in, and the website will take a look and try to match you up with a celebrity. And it's stunning to see

how close people could be to a real celebrity, and make you realize there's an awful lot of us that look the same out there and I don't know if facial recognition will work.

There is some research being done on intelligent CCTV that to me, at least, appears to be mostly traffic flow. It's looking for the person that's walking, you know, out the entrance door or trying to go to a door that's in a secured area so, you know, the minority report type things I haven't seen yet, but that's -- who knows when that will happen.

We did do a request for information to industry to try to get the state of CCTV and see what comes back. We have another program. It's SPO. It's a device that measures passive millimeter wave energy off your body so every -- every individual produces this kind of energy.

And these cameras look for that, look for interruption to that energy. The image is identical to CCTV so it's really nothing. The viewer is not seeing anything different than what they would see if you were just walking toward them, but there is a bar graph on the side that goes green or red depending on whether there are large areas of your body that are -- energy is being interrupted.

And then that may lead to a person being asked to, you know, open their jacket to show they are not wearing a bomb. That's basically what it's addressed for, suicide bombers. There are some pilots that have taken place in the past at rail stations and at a ferry, and just currently one in an airport.

We have our behavior detection officers. There's been some press coverage of this already, and there's a fair amount on the TSA website, and these are people that really are doing the same sort of thing that a lot of stores do, retail establishments do, and that the police have always done, which is what doesn't seem right here.

They are looking for behaviors that are indicative of tension or fear or deception, that sort of thing. Many people say that's every single person at the airport, but they will look for these factors.

And if you reach a certain threshold, then you may be asked to undergo a secondary screening. In terms of a result, every individual is subjected to a secondary screening on a random level anyway so I don't know if there's all that much difference in terms of what the individual will experience, but if it's high enough, then law enforcement will be called over.

And law enforcement will conduct an interview to try to resolve what it is that's causing you to display these behaviors. And if they are able to resolve it or unable to resolve it, but there's nothing else -- you are not carrying a gun or carrying drugs or other things, which is typically why we found people to be displaying these behaviors, then you are free to fly.

So far the program seems to have caught, quote, unquote, illegal immigrants, drug smugglers and individuals with fraudulent documents, including some that have had 75, 80 credit cards in different names. One last week with \$900,000 cash and crystal meth in their bags.

The program is not looking for those things. They are looking for the behaviors. Unfortunately, the behaviors they are looking for are also typically associated with criminal activity. And so if they find it, they are not going to turn a blind eye to it, but that's not the target of what they are looking for.

They are looking for the behavior and trying to resolve the source of that behavior. The program is also based on a long history, I guess, in some other countries, including Israel. And like I said, the experience of retailers -- I've spoken to some store managers who can tell you right away if somebody walks in a store that they aren't there to shop. They are there to shoplift.

And when you ask them how to explain what the source of that is, it's just years and years of experience. I think that's what they are trying to build off of.

And the last one I want to talk about is some of the efforts that some of the airports -- and this is still a pilot program to make sure that the documents that you are presenting are authentic, and that includes the boarding passes, which was the subject of some media coverage, I think, last year where an individual said here is how to create your own boarding pass at home and put whatever information you wanted to it.

We have a hand-held device now that will read the boarding pass to make sure that the max strike on the back of the boarding pass or the bar coding on the front of it -- the information that's on there actually matches what is on the face of the boarding pass.

And then once it's been read and confirmed, then, the information disappears from the device. And if it's not read because it is fraudulent, then it still disappears. And we rely on other enforcement measures, but the device itself doesn't capture the data.

That's kind of the privacy protection we tried to build in. There was no data captured in this system. The other thing we're doing is looking at the identity that people present when they travel to make sure that the identity cards are authentic and haven't been tampered with.

So it could be anything from a passport that turns out, you know -- if you smudged the ink a little bit and it rubs off and you find out that it's fraudulent or, you know, it's completely fake identity, driver's licenses, things like that.

And there are also going to be a hand-held device that's going to take a look at the minutiae on those types of card to make sure they are valid. Again, the price of protection

here is the hand-held device is not capturing any data. It's looking for minutiae to make sure it matches.

If a California driver's license has a certain type of font on it, then that's the font that this thing will read, and then it disappears again. So that's kind of where we are and different things, both internal in terms of protecting our information, that we do collect, and external in terms of programs that really affect the outside.

It's a constant effort because there's an awful lot going on. And we are trying to hire more, but it's hard to find good people. And I am open to any questions.

MR. BEALES: All right. Thank you very much, Peter.

Jim Harper.

MR. HARPER: Thank you for your summary. Very interesting. A lot you've covered. As you were speaking, I ran your picture and mine through findmycelebritylookalike.com, and the technology is not ready for prime time.

MR. PIETRA: I don't know where you got my picture. I don't think it's out there.

MR. HARPER: It's on CNN news, actually.

MR. PIETRA: I remember that one.

MR. HARPER: Some bad picture, but it's the only one I came up with. You mentioned -- maybe not a transitioning away from database security, but an acknowledging of the weakness of identity-based security, the idea of behavioral approaches, behavior-based security.

And I wondered if you could describe in a little more detail or cabin what you mean by behavior based because that could involve a range of behaviors, anything from a deep dive into a person's, you know, finances, medical activities, spending, et cetera, all the way up to sweating in the airport or what kinds of behaviors are you talking about when you say behavior based?

MR. PIETRA: When I talk about behavior based -- thanks for giving me an opportunity to try to clarify because I don't want to cause widespread panic, but the behavior-based conduct would be things in the airport or things even that -- maybe from the parking lot. I'm not sure.

I don't think there is anything out there in the parking lots right now, but these would be things inside the airport; not looking at your background, beyond what I call the identity base checks, when you placed your reservation, and it would bounce against a wash list and be conducted by Secure Flight.

MR. HARPER: Physical activities in and around the security area?

MR. PIETRA: Right.

MR. HARPER: Consider your repeat focus on devices and programs that don't keep data for very long. I think that kind of stuff, if it works, could be done quite privacy protectedly, if it disposes of data quickly when there's nothing interesting happening.

MR. PIETRA: I hope so. The document checker and the boarding pass is immediate. It's not stored. Once you pull it out, it's gone so I'm very happy with that. Secure Flight has a very short retention period as well, seven days for what's going to be the vast majority of travelers.

Anyway, his name doesn't actually come up as a possible match to the wash list, and that should be -- that should be two million passengers a day that we'll keep their name for seven days and then they are going to be gone.

MR. BEALES: Could I just follow up briefly on the behavioral stuff? How does the communication work to designate somebody for secondary screening? I mean, presumably behavioral surveillance is out in the line or before you approach security, even somewhere else in the airport.

And as I understand it, the boarding pass is the main mechanism of identifying who's got to be -- who is going to be subjected to secondary screening. And I don't know how you get the information from the behavioral surveillor to the person who's got to pull you out of the line and into the secondary screening line.

MR. PIETRA: Well, it can be as low tech as a fingerprint. This is the person that --

MR. BEALES: If it's right there, sure.

MR. PIETRA: Correct. And that's -- you know, there were some scary -- what I consider scary proposals. Take a photograph of a person that is the subject of an interest and then pass that photograph on to, you know, the next person so they can know that's the person they are supposed to do a secondary screening for.

In many respects, that's nothing more than an electronic fingerprint against -- this is the guy. My concern had been, well, what are you doing with that photograph? Are you storing it? How long are you storing it?

All the of rest that, that is something that -- those kinds of conversations, you know, for now, at least, have killed that idea, but typically it is a matter of the person that is making that behavior assessment saying, okay, well, that person is doing something that raises my alarm.

They have a score sheet, basically, to identify behavior. At that point the person is still anonymous to them. They don't have a name. They don't have anything. In fact, there was some discussion about whether you could go up to that person and ask them

their name, and we decided no, you can't, until they get into the actual checkpoint, into the screen -- are undergoing the screening process.

And so I can't remember now whether there are things like a description of the clothing they are wearing so that gets passed on so there can be kind of a hand-off to somebody else, but that's basically the process. It's a low-tech technique, but it's a fingerprint.

In some cases, you know, the effort is to put people at ease and I think the Israeli model is a little more to put people at unease to reveal their behaviors. I think the TSA method is to kind of put them at ease so it's a very casual conversation. How are you?

How are things going? Where are you flying? How is the weather there? And that sort of thing. And they are not looking for what the actual substance of the answer is. They are looking for the behaviors that are accompanying the answers.

And that conversation will take place in the line as they approach a screening checkpoint so when they get to the front they will be able to tell the person that's checking the documents and puts a little mark on your boarding pass that, yes, someone needs to be screened or not.

People who get selected for secondary screening are not always designated by the boarding pass. It can be a more random process than that. It could be also people who -- I even, you know, because I have a metal head plate, every single time I walk through a magnetometer, I get the secondary screening every time I fly.

MR. BEALES: Renard.

MR. FRANCOIS: I, too, wanted to ask you about the behavioral screening. I have two questions about it. And the first is -- I'm not sure if you are at liberty to discuss this. If not, please feel free to let us know.

The first is what organization or who is doing the training of the agents to do that because you made reference to Israel a couple of times and I know that that has been particularly effective.

And so are you working through a private company or are you partnering with other countries to have some sort of partnership where their agents are training TSA personnel to do that?

MR. PIETRA: No. Actually, it's funny. A lot of other countries are asking to see our training protocols, including Israel because we actually don't get the training from them. Their program is a little different, but I mention Israel only because the idea of using behavior detection is something they have done a lot of work on.

We do it in a different way, though. But a lot of the work comes out of the work done by a guy named Dr. Eckman, Paul Eckman from San Francisco who has been doing this for about 40 years, but the actual training is conducted by TSA. And some of it was developed within DHS, within the SNT component.

MR. FRANCOIS: And my second question is have you contemplated working with the airlines so to -- at least offer some sort of training to not necessarily gate agents, but people at the ticket counter so at least the behavioral observation can be done a little earlier than in the line?

MR. PIETRA: I don't know. I don't know the answer to that. I do know that there is a concern that the training -- first of all, it's pretty sensitive. It's a two-week straight block of training. And if you interrupt that block, then you are out of the training and you have to start all over again.

There is concern that the techniques don't become too widely available. Among the countries that have asked for the training have been Iran and Syria. And so we -- I think we so far have been reluctant to share the training with them.

So I don't know the answer to whether we have talked about expanding it to the airlines. And it's not -- like I say, it's not an easy training. And what you really are trying to make sure is that you are looking for certain behaviors and not allowing any kind of internal predilections that you may have influence your judgment. So -- because then it really invalidates what we're really looking for.

MR. FRANCOIS: What do you think the eventual scope of this is? Is it to have all TSA agents trained in this?

MR. PIETRA: No.

MR. FRANCOIS: Just kind of a certain few for each airport?

MR. PIETRA: Yes. It's the latter. I don't think it's something that -- because it does require a concentrated effort. It's not the kind of thing you can do kind of on the fly. The individuals that are doing other kinds of security screening that we do at the x-ray machinery or things is -- it's not an option for them to do that.

The other thing is that there's some question about how long can these individuals do this job before they have to be rotated out so they don't become stale. And that's something that they are looking at as well.

MR. BEALES: Richard.

MR. PURCELL: Peter, thanks for being with us today. We've talked about your work or developments over the last year in the TWIC program, whole body imaging,

surveillance, passing micrometer wave measurements, document verification. Like the others, I seem to be settling on this risk assessment by walking around issue.

I only have one question. Should an assessment create a secondary screening? Should that screening create a further interviewing and perhaps involvement of law enforcement?

Does TSA receive reports on the individual, named individual for those circumstances? And if so do they database those reports? And if so, do they retain those reports for a specified period of time?

MR. PIETRA: At this point, the only time that PAIs are taken is if law enforcement is actually called over and if they make a report. So TSA does not independently take the information. If they do, then, yes, it does get databased. It goes into our -- well, it goes into our TISORS 01 system of records, which is our enforcement system of records, and that covers, among other things, any kind of suspicious activity at a checkpoint or any kind of a security screening effort.

Now, we also take statistical information. So for all those individuals that are not -- that we do not take an PAI from, for all those reports that we generate, well, you know, we see somebody that, you know, has a certain indicia, then we do a statistical report for that.

And that is briefed weekly to say, well, you know, what are the types of things that we are -- what are the types of behaviors that we are seeing that may cause some concerns, but it's not tied to the individual. We don't have their information.

MR. PURCELL: So let me just follow up with that. I've got to understand what this means. So a person is in line. They appear nervous. They are jittery. They are anxious. First, they have a conversation with a behavioral detection officer, go to secondary screening as a result of that and are not clear or are somewhat incoherent in terms of the answers they give.

Officers -- law enforcement officers get involved and it turns out to be somebody who's incredibly distraught because a relative has passed away, a mother, a father. They may be late for their plane and they are only getting increasingly distraught.

As a police officer, I would probably want to file a report on that, not for any other reason except to cover my own career by making sure that I documented what happened because this person is distraught and there may be a complaint, and I want to make sure that's on record. Would TSA keep a record of that then?

MR. PIETRA: If the law enforcement officer makes a report, then, yes. I don't know what the protocols are within the various jurisdictions and what it is the law enforcement officer would use to trigger -- you know, write his report. But if the law

enforcement officer writes a report, then we would get -- we would keep that incident report as well.

MR. PURCELL: And your retention period then?

MR. PIETRA: I don't know off the top of my head. We have a PIA for the system. It's internal. It's informal clearance. I can't remember now what it was. The hard copy reports are destroyed as soon as the data is entered electronically, typically within a day, but I can't remember how long the electronic records are kept.

MR. PURCELL: I'm more concerned about the electronic records in your system of records. If you don't mind, I'll follow up with you offline and if you find out what that results in, let me know. Thanks.

MR. BEALES: John Sabo.

MR. SABO: Just following up on that, Peter, one of the principles in our committee, principal framework is efficacy. And if I'm not mistaken, and correct me, but I think the primary reason for secondary screening is to ensure that the traveler is not carrying a concealed weapon or doesn't have a physical means to disrupt the flight or crash it or -- correct?

MR. PIETRA: Yes.

MR. SABO: In the efficacy principle, it seems to me, if you do the behavior stuff or whatever you do, and then you go through secondary screening, nothing is found, the flight proceeds without incident, what possible purpose would there be to retain the data under any circumstances, since the whole purpose -- this gets to the whole issue that we create systems for a purpose.

Then the bureaucracy of the system creates ancillary data reports in pieces of the system that gets retained irrespective of the outcome. It would seem to me, in that sense, the purpose would be -- you know, someone may be distraught, whatever the reason.

There are a lot of human reasons to be upset. If the flight proceeds without incident, that should be wiped off the map because there was nothing found. The flight wasn't disrupted. Do you see what I'm saying?

MR. PIETRA: I understand what you are saying. Again, remember that these records go within this enforcement system that retains -- it's the same issue with all those, all those records.

You know, if you come through a checkpoint without any PEO involvement and you have a pocketknife on you and it gets taken, and you go on a plane and fly, that record is going to be retained just as long as this person that raised the hackles of a BDO -- and the idea that the person made the flight and the flight was -- nothing happened on the

flight and therefore that's the end of it. It should be gone. I think it ignores the issue of people who test the system.

MR. SABO: The distinction is that somebody had a weapon -- well, what's perceived as a weapon, but it is a physical instrument that's banned, but where a behavioral identifies someone. Nothing is found. There is no interception of anything.

MS. MCNABB: It's another explanation, in fact.

MR. SABO: Correct. So I guess I'm saying I can understand the example you used because you actually have something that's prohibited. And it could have been someone testing the system that might have used it.

MR. PIETRA: We get -- we get guns almost every day loaded, unloaded. We get -- we had one recently, a block of cheese, a hard block of cheese with wire wrapped all around it. The guy said, oh, I wanted a safe way to wrap my iPod ear plugs. It seems kind of odd.

If they, then, are stopped six months from now with the exact same thing, then you've got to start to think, well, you know, this is kind of an odd thing. Now, that's where you get to, you know -- how is this to be used?

Okay. The person comes through the system, has no issues. The plane flies. There's no enforcement action. Then the data is there. Nothing has happened to that individual. But let's say he does the exact same thing a couple months later. He does the same thing next day at a different airport.

Then you may have a trend that you would want to investigate to see whether this is an individual that is testing the system. You're not going to know that unless you retain that data for a certain period of time. I don't know what that time is. I don't think it's long.

MR. SABO: All I'm saying, the block of cheese attack methodology, which may be repeated multiple times, for some reason you may feel that could be potentially a model for a threat, but that's a lot different from a behavioral.

MS. MCNABB: Misread.

MR. SABO: Misread.

MR. PIETRA: Right.

MR. SABO: I mean, theoretically you could have a disgruntled passenger who hates coming to airports, is always disgruntled.

MR. PIETRA: Right. A lot of those get resolved short of law enforcement. We do get the individual that comes in and says I am late for my flight. Which Ken just reminded me I'm about to do it. Good thing it's across the street. So I need to go. So I will

take a look at exactly what that potential period is and send it to you all. I don't recall what it is off the top of my head, like I said.

MR. PURCELL: That would be great. It would be interesting, also, if you can talk to whoever is managing BDOs, talk to them about how often law enforcement might make that kind of report when it's a distraught individual as opposed to somebody who is breaking a posted rule.

MR. PIETRA: Right. Okay.

MR. BEALES: Thank you very much, Peter. We appreciate you being here. We wouldn't want you to miss your flight.

Our final speaker today will be Alfred Campos, the Assistant Field Director of the El Paso Processing Center. Mr. Campos has 25 years of INS and now ICE law enforcement experience with the Border Patrol as an immigration inspector, as a supervisory inspector, a deportation officer, assistant officer in charge, the officer in charge and an assistant field director.

He's served several extended details to Washington on special projects, and he has a BS in criminal justice from the University of Texas at El Paso. Thank you very much for being here today.

MR. CAMPOS: Thank you very much, distinguished panel. And before I continue I would like to introduce our Deputy Field Officer Director who was able to join me, Mr. Francisco Venegas. He's our Deputy Field Officer.

MR. BEALES: Welcome, and thank you for joining us.

MR. CAMPOS: I trust the tour was very good yesterday.

MR. BEALES: The tour was wonderful. I should say this to you and to the staff. This was a tremendous field trip. And I think we all really appreciated it and felt like we learned a lot about what the world looks like from your point of view, which is real useful to us.

MR. CAMPOS: Very good, sir. Thank you very much. Briefly, I've been asked to speak on behalf of Detention and Removal Operations under Immigration and Customs Enforcement about our border operations and how we work with the other agencies, and basically what we do. And I've been given half an hour, and we'll see how short I can keep it.

I will start off with our field office here in El Paso is run by Mr. Robert Charoff (sic). He's the Field Office Director. Mr. Venegas is our Deputy, and we have six assistant field office directors out in the field operating from Pecos, Texas, which is about 175 miles to the east, and Albuquerque, New Mexico, about 270 miles to the north. And that is our

entire geographic area; 15 West Texas counties, El Paso, Texas and the entire state of New Mexico.

We work closely with the local agencies to accept and detain individuals who have been arrested, Customs and Border Protection, El Paso and Marfa sectors, and locally the El Paso Office of Field Operation at the ports of entry as well.

We also work with the Office of Investigations here under Immigration and Customs Enforcement. And our main facility is the El Paso Processing Center, the one you toured yesterday. That has a capacity of 840. It can go up in an emergency to 1,100 or 1,200.

We have roughly, like you saw in the attachment, about 75 different nationalities, 40 percent criminal and the rest are non-criminal from a variety of countries. We have four courtrooms there that can handle administrative hearings.

And we also utilize other tools that Congress has given us going back to the 1996 Act and we can administratively remove detainees that have been identified when they fall under certain requirements of the law. And that has really helped us to remove a lot of detainees from the country.

We also receive detainees at a regional level. We accept detainees from the entire state of Texas, other facilities that may not have room, up to Denver and Los Angeles. And we also receive from the east coast to help alleviate the lack of bed space out there.

And we transport that through coordination through Washington, D.C., which is the Justice and Prisoner Transportation Program. That is run pretty much by the Marshal Service. Currently we have ten aircraft that move detainees across the country, and we receive detainees through JPTP almost on a daily basis, Monday through Friday, sometimes on Saturdays.

We take detainees as far north as Washington State from our facility in the Seattle Field Office, and as far south as LA, again, and through Denver and Idaho, and wherever the aircraft is required and needed to pick up detainees and bring them south.

It expedites moving them through El Paso. The majority of our removals are through Mexico. And we coordinate all of our removals through Mexico with the Mexican Consulate here in El Paso and Mexican Immigration.

We have -- operationally, we have in Pecos -- they operate what's called the Criminal AD Program, and there's a facility in Pecos that has 3,500 inmates under the Bureau of Prisons, and pretty much 100 percent are all immigration violators from various parts of the Southwest.

There is also -- in Albuquerque, there is also the Seagoville Correctional Center, and we get detainees from that facility as well. And then here locally we have the Federal

Correctional Institute in LaTuna at the Bureau of Prisons, and that has, approximately, close to 2,000 with a satellite facility as well.

We operate in these facilities to identify and put through proceedings and remove out of the country as expeditiously as possible. Many times they end up at our processing center to either see a judge or to await removal.

Awaiting removal can be a tricky situation because we have to coordinate the removal or the deportation with that country, the foreign government, the consulate or the U.S. Embassy, depending on which nationality it is.

The majority of our removals are from Central America and, of course, Mexico, but we do have most of the consulates that have their jurisdiction in El Paso, there, the Houston office and Washington, D.C. for some of the embassies.

Currently we have approximately about 360 government employees in the El Paso Field Office and roughly 400 contract employees employed by the El Paso Field Office. The contract employees are guards for the facility.

We also have the U.S. Public Health Service, and they are the Division of Immigration and Health Services providing medical care for detainees at the facility. We also have a small staff of Northrop Grumman computer specialists.

And the most recent contract acquisition has been Aetna. And they provide food service operations at all the processing centers for ICE across the country. Aside from removing individuals by land here through El Paso into Mexico, we remove through, again, the JPTP aircraft into Central America.

And we have several flights on a weekly basis or every other week, depending on nationality where we can get the nationality that we have in hand and expeditiously move them and save the government money by utilizing JPTP as opposed to removing by commercial air, which we also do on a regular basis.

Commercial aircraft is mainly used for other continents that it's really difficult to get a removal on, but we do, again, work with the consulates and the embassys to remove these detainees.

We also coordinate with the State Department so that they are aware we are arriving and how many officers are escorting and who is being taken back home. And we advise them of this. The El Paso a processing Center as you saw, is, in my opinion, of course, one of the better facilities ICE has.

We are accredited by the American Correctional Association and the Joint Accreditation for Correctional Health Care Organizations, and the National Accreditation for Correctional Health Care. There's three accreditations that the facility has garnered.

I must say our last one we received a high score of 99.4. We only failed in two standards, and one was, as miscellaneous information, one of the compressor issues and another was one that we just could not simply physically meet. And we are working to try to physically, through construction, meet that requirement.

We also have an initiative that we started last year, the Criminal Alien Program. Our enforcement agents were upgraded about three years ago from detention enforcement officer to an immigration enforcement agent, which gives them the statutory authority to interview, identify and prepare aliens for either removal proceedings and/or even prosecution.

The Criminal Alien Program is to establish, to identify any foreign-born national in any local state or federal facility and initiate the removal process based on statutory requirements.

We currently operate out of the El Paso Detention Facility. It has an annex in east El Paso. They have roughly a population of about 2,000 combined. We also have a state facility out east of the city and, of course, the federal facility that I was referring to.

We have also initiated, most recently, a prosecution program where we identify some of the individuals that have violated, of course, immigration law and be subject to criminal charges. And we are working with U.S. attorneys, and we are now presenting cases for prosecution, but the majority of our work is to identify the foreign-born nationals who have committed crimes in the U.S. and deport them as efficiently as possible.

And we also have other tools that help us to remove detainees or aliens. We have what's called the reinstatement where if an alien was ordered deported previously, we could reinstate that order, thereby reducing the time for any hearings or any other issues. We just reinstate the issue and prepare for removal.

And last we also are the main office for the Mexican Treaty Transfer with the Bureau of Prisons. Treaty Transfer Program is between both Mexico and the U.S. and prisoners in both countries or opposite nations apply for this program.

And after they have gone through a rigorous Bureau of Prison test, then they will be eligible for the program. And they are -- basically their sentence is reduced in the U.S. by being sent home, deported, but they complete their sentence in their home country, in this case Mexico.

We just went through one recently. We do it every three months, and usually we get anywhere from 30 to possibly 40 Mexican nationals, and about ten percent of those would be females. And we receive from Mexico approximately half that in U.S. citizens, which, again, five or ten percent would be females. And most of the American citizens are extremely happy to return home and serve their time in the U.S. prisons. And that, in a

nutshell, gentlemen, is basically what we have. I know Mr. Venegas would like to share a few thoughts, but again we would be open to questions.

MR. VENEGAS: That's very good of you. I'm pleased to be here. I was a last-minute addition. Sorry I didn't get you my information. Nonetheless, it is my pleasure to be here to address this distinguished committee.

Mr. Campos has done a fairly good job on touching on all the activities that we become involved in the removal of people that are determined to be in this country illegally. I think in his brief overview you can see that we have contact and info sharing with many other entities, both law enforcement and non-law enforcement.

And we take very great care in understanding what information can be shared and when it cannot be shared, as it's important to us to understand that we are, in most cases, dealing in administrative removal-type cases, not criminal cases.

Even though we deal with criminals, at the juncture that we are involved, they are administrative violators. And we hold true to that belief and carefully guard any information that may be disseminated.

Once again, as he stated, our priorities are, at this time, Criminal Alien Program, the detention of aliens and also fugitive operations. So our focus has turned toward the criminals and getting information to make those necessary apprehensions so we can remove the criminal element from our society, reducing the risk of terrorism, as well as criminal violations and threats to the general public.

That is our focus, but we have many tools that we utilize, the biometric database and the like, and once again, we adhere to many strict guidelines established through DHS and ICE, and federal and state government entities to ensure that our practices are adhered to.

We do that with our staff by conducting training regularly, two to three times a year, through various modes, whether it be in person or whether it be through the electronic media now that we have a virtual university established within our ICE program, but constantly training and education is something that we focus on to ensure that people understand the privacy of information and the guarding of that information is utmost priority within our organization. And we will field questions now

MR. BEALES: Thank you very much. Neville Pattinson.

MR. PATTINSON: A quick question about biometrics and use of biometric databases. And, first of all, I should say thank you very much for visiting us today. It was outstanding and very informative and your staff is to be complimented for their openness and willingness to share and answer questions. So, again, thank you for that.

So coming back to biometrics. We saw people being processed yesterday. To what extent they are coming in with fraudulent identities, fraudulent documents and so on, are biometrics helping determine repeat offenders as far as somebody coming under a completely different identity and you don't discover them?

You've been here before but you were called so and so last time. Is that helping or is it the biometrics that you are using to catch them and just prove that they are the same person coming back with the same identity? What is the purpose of biometrics?

MR. VENEGAS: Actually, you hit one of the main purposes, to identify those that want to use fraudulent names or fraudulent documents by using, for example, the IDENT System and others, all those systems have proven to be valuable tools in positively identifying an individual, regardless of what name, date of birth or country of origin that they claim to be from. So biometrics has definitely been one of the most important tools we've had provided to us.

MR. PATTINSON: As a follow up, you obviously enroll them or validate their fingerprints when they are processed for the first time. When you release them, do you verify the biometrics again before they go so you know you are releasing the right person?

MR. VENEGAS: Correct. And Mr. Campos is more familiar with that so I'll allow him to address that.

MR. CAMPOS: Most definitely. Every detainee that is brought in and is to be booked in, of course, they probably have already been enrolled by the apprehending or arresting agency. And we just verify that. And we'll recheck upon their departure because sometimes our detainees can stay with us.

We had one detainee one time that stayed with us close to five years because in our process they could appeal the judge's decision to the BIA and to the circuit and then, of course, to the Supreme Court so within that time frame another warrant might have popped up, but, yes, we do check. And we do get a lot of warrants, and believe it or not a lot of states don't want some of these smaller, petty crimes that they happen to have a warrant out there for them so -- but they just kind of note? In their records that they are in immigration detention and they will probably be deported, and they close their records out that way.

But we do use the system if we need to remove anybody completely because we do make arrests and we do take them to the facility or we use the IDENT system just to verify and to enroll or to remove, to put them through the system

MR. BEALES: Jim.

MR. HARPER: I suppose it's axiomatic that the time you spend with the civil violator, that is someone who is just in the country illegally, which I understand is a civil

not a criminal violation, at least the first time -- the amount of time you spend with the civil violator takes away from the time you spend with the criminal violator.

But to get a sense of what percentage or proportion of time you spend on either one, do you have a number or anything close to it on how much time and how many people you are dealing with that are civil violators who don't have a background of criminality compared to the ones who do have violence and thievery and so forth.

MR. CAMPOS: Yes. Like I said, 40 percent are criminal so 60 percent are non-criminal and our length of stay at the facility is roughly about 41 days. Criminal aliens usually, for the most part, they are coming out of another facility, either it's a state or a federal, and they just want to go home.

And if they -- if they didn't have to go to see the judge, you know, they would really -- I mean, because a lot of them we can administratively remove because they are illegal and we can use the administrative removal tool.

So we do -- as far as taking time, I guess, in processing and attending to the non-criminals, it doesn't affect that much because operationally in the facility we just need to separate them and manage them all the same. The judges have their courts and their dockets.

A lot of times the criminal ladies are the ones that end up taking more time because they want to try to right their case and that's where the dockets and the merit hearings are extended for several times. And a lot of times some of these may even want to go for political asylum for another continent that can try to use that angle.

MR. HARPER: And do you see trends over time with the amount of civil versus criminal or do you know all the talk among people who don't deal with this daily is that illegal immigration is at all time highs. Are you seeing simply more civil violators than you have in the past or does it -- is it affected by U.S. law, by enforcement efforts? What causes any changes in the population that you are dealing with?

MR. VENEGAS: I think the philosophy does have a lot to do with it. Our focus has really geared toward criminal offenders that are fugitives within the United States. You hear about this overwhelming population that's roaming within the United States.

We as an entity, as DRO, are targeting more criminals, but you will always have the civil violators because that is the majority of people apprehended at the point of entry.

The violators, criminal violators, are either being identified in institutions or correctional facilities or they are being caught through our fugitive identification program, which puts them as a priority of people that we are looking for versus the civil offenders.

MR. HARPER: Thank you.

MR. BEALES: Anybody, any other questions? All right. We want to thank you again for our wonderful tour of the facility yesterday, and thank you both for being with us today. We really appreciate it.

MR. CAMPOS: Thank you very much for having us.

MR. VENEGAS: We appreciate it.

THE COURT: I believe we established in our administrative meeting at lunch that we didn't have any subcommittee reports. And that leaves us with the last item of the day, which is public comments. If anybody signed up for public comments or would like to sign up for public comments, now is the last chance.

And failing that, I want to thank you all for your time in El Paso. I think this has been a productive session and I look forward to seeing you all again in June. Meeting adjourned. Thank you.

(Proceedings concluded at 2:52 p.m.)