FDCH TRANSCRIPTS
Congressional Hearings
Sept. 30, 2004

House Select Homeland Security Subcommittee on Infrastructure and Border Security and Subcommittee on Intelligence and Counterterrorism Hold Joint Hearing on Disrupting Terrorist Travel

LIST OF SPEAKERS

CAMP:

The joint hearing of the Subcommittee on Infrastructure and Border Security and the Subcommittee on Intelligence and Counterterrorism will come to order.

The subcommittees are meeting jointly today to hear testimony on the Department of Homeland Security's efforts regarding terrorist disruption of travel.

The purpose of this hearing is to look at the recommendations made by the 9/11 commission report and examine DHS's effort to obtain, analyze and disseminate terrorist travel information.

On the first panel, we have General Patrick Hughes, who is the assistant secretary for information analysis, and Assistant Secretary Stewart Verdery from the Border and Transportation Security Policy Office.

On the second panel we will hear from Professor Lawrence Wein from Stanford University who will provide an overview of research he's done regarding the US-VISIT program.

I would like to officially welcome all of our witnesses.

I ask unanimous consent that member opening statements be included in the hearing record and encourage members of both subcommittees to submit their opening statements for the record.

And because this is a joint hearing, members will be recognized based on order of appearance.

Having said that, I will submit my opening statement for the record.

At this time I would recognize Mr. Gibbons, chairman of the Intelligence and Counterterrorism Subcommittee, and is now recognized for any opening statement he may have.

GIBBONS:

Thank you very much, Chairman Camp.

To our guests today, welcome.

General Hughes, it's great to see you back before us.

And Assistant Secretary Verdery, thanks very much for your presence here as well today.

It's an important hearing we're going to have today. I know that your testimony is very valuable. I, like Chairman Camp, am going to follow his lead and put my opening statement into the record so that we can move along quickly and expeditiously so that we don't take more of your time.

I know that you're both facing immense challenges right now. It's an exceedingly important job, and we look forward to hearing your testimony today.

With that, Mr. Chairman, I'll submit my testimony for the record.

CAMP:

Are there any other opening statements?

I think at this point we'll go to our witnesses.

I, again, would like to thank them for being here.

General Hughes, we'll begin with you. We've received your written testimony and we'll ask that you briefly summarize in five minutes your statement.

Thank you.

HUGHES:

Thank you very much, and good day, Chairman Camp and Chairman Gibbons and distinguished members of the committee, the joint committees.

As you know, the Department of Homeland Security was envisioned, formed and is now in operation. President Bush's decision to establish the department has enabled us to unify our diverse resources into one team to prevent terrorism in the homeland, to ready ourselves against our enemy and to ensure the highest level of protection for our country and the citizens we serve.

Through the Homeland Security Act of 2002, among other things we are charged with integrating relevant information, intelligence analysis and vulnerability assessments, to identify threats, to inform preventive priorities and to support protective measures.

We are doing this in partnership primarily with federal partners and state and local governments, agencies and other organizations that we find at the state and below level and with our partners in the private sector.

The Office of Information Analysis, which I represent, is the heart of intelligence at the Department of Homeland Security. It is responsible for accessing and analyzing the entire array of intelligence related to threats against the homeland and making that information useful to our federal partners, first responders and anyone in the United States who can use that information and has the right to receive it.

IA provides a full range of intelligence support to the secretary and DHS leadership and to all of our components.

Additionally, IA assures that the best intelligence information available informs the administration of the homeland security advisory system.

In order to perform these duties, we must receive intelligence from a number of sources, including not only the United States intelligence community and our state, local, territorial, tribal and private sector partners, but also from the Department of Homeland Security entities with intelligence capabilities.

The large amount of information we coordinate includes reporting from the United States Secret Service, the United States Coast Guard, the Border and Transportation Security Directorate, Immigration and Customs Enforcement, including the Federal Protective Service and the Federal Air Marshal Service, and Customs and Border Protection, the Transportation Security Administration, the Office of Citizenship and Immigration Services, and the Federal Emergency Management Agency -- 180,000-plus persons on the ground throughout the country acting as eyes and ears, enforcers and workers, and policy-makers in some cases, in order to protect the country.

We represent a primary element of the United States intelligence community, a powerful source of information and a powerful capability in order to use the information we have to protect our citizens.

We have a sense of purpose and we have embarked on what has likely never been done before with regard to information fusion: to fully understand the threat and the conditions that make that information useful at a utilitarian level for such a broad range of officials -- from city mayors, to border patrol agents, to airport screeners, to critical infrastructure operators, to the cop on the beat.

This concludes my oral statement. I'd be happy to answer any questions you have today. I'm looking forward to our interaction.

Thank you.

CAMP:

Thank you very much.

Mr. Verdery, you have five minutes. We have your written statement, and if you could summarize it that would be helpful.

VERDERY:

Of course.

Chairman Camp, Chairman Gibbons and other members of the committee, thank you for the chance to be here today to join with General Hughes to testify about the efforts of the Department of Homeland Security to analyze and disrupt the travel of potential terrorists.

The 9/11 commission noted that, and I quote, "Targeting travel is at least as powerful a weapon against terrorist as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators and constrain terrorist mobility," end quote.

The administration and this department concur with this observation, and we have implemented a number of successful programs to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators and constrain their mobility.

This is a complex, multi-agency undertaking, and we're working in close collaboration with our interagency partners on this important task. We're reviewing how travel documents are produced and reviewed so we can better detect altered and fraudulent ones, improving and expanding watch lists, and exploring ways to share data with our foreign counterparts that can help identify and thwart terrorists.

And of course, these efforts are designed to protect and respect the civil liberties and privacy of U.S. citizens and residents and our visitors.

I believe General Hughes, in his written testimony, ably described the role of the information analysis section of DHS in participating in the intelligence community. It's absolutely critical that actionable information be provided to the front-line components of DHS, whether it's an inspector at a port of entry, a federal air marshal, an aviation screener or a criminal investigator, and that capability is robust and improving.

The BTS directorate is the current operations unit responsible for ensuring a continuing productive relationship between the intelligence arms of BTS -- that's Customs and Border Protection, Immigration Customs Enforcement, and TSA and IAP.

BTS analysts are assigned to IA, and there's a daily exchange of information between BTS agencies, IA and of course the Coast Guard.

BTS analysts conduct follow-up research involving BTS incidents of interest and its intelligence community. And we've essentially set up a two-way street of information-sharing where our components receive information immediately through IA, and IA is immediately alerted to significant operational activity.

Let me focus briefly on some of the programs we think are really disrupting the patterns of terrorist travel, and I'll focus on the National Targeting Center, the US-VISIT in our effort to find fraudulent travel documents.

The National Targeting Center operated by DHS' U.S. Customs and Border Protection, working with numerous federal agencies, provide tactical targeting and analytical research support for passenger and cargo targeting in the air, sea and land operations in inbound and outbound environments.

NTC develops tactical targets, potentially high-risk people or shipments, that should be subjected to additional scrutiny by CBP personnel from raw intelligence, trade, travel and law enforcement data via the automated targeting system, the ATS.

NTC supports the DHS field elements, including our container security personnel in 25 countries around the world, our visa security officers in Saudi Arabia, the CBP officers at ports of entry and the border patrol, and it's also working to support the pilot immigration security initiative, the ISI, operating in two airports in Europe to work on vetting passengers before they leave for international flights.

During the heightened threat period last December and throughout the winter, NTC played a pivotal role in analyzing advanced passenger manifest information related to several international flights of interest that were deemed to be at risk in order to secure those flights.

DHS is committed to improving the collection of manifest information over coming months by standardizing formats, requiring departure information for outbound flights and finalizing crew manifest requirements. And these requirements will build on the passenger name record, so-called PNR data, used for screening passengers.

I personally served as the lead negotiator for the U.S. in our successful negotiations with the European Union to now allow that data to be transferred from Europe to DHS for analyzing incoming passengers.

The US-VISIT program is a continuum of identity verification measures beginning overseas with the visa-issuance process operating at 206 non-immigrant posts, 118 immigrant visa-issuing posts, 115 airports and seaports of entry.

Secretary Ridge I think deserves great credit for moving ahead with the biometric component of the system ahead of schedule.

And just to briefly summarize, as of the first nine months of operation, we've now detected I believe 838 individuals identified by the biometrics alone at ports of entry as subject to a watch list information or other lookouts, and about a third of those have had adverse action taken against them -- being refused entry or being arrested.

In addition, today, September 30th, is the first day that travelers in the visa waiver program are being enrolled in US-VISIT.

The commission's report noted that terrorists use altered and counterfeit travel documents to evade detection. Just yesterday I toured the ICE Forensic Document Lab in Northern Virginia who have accumulated 130,000 legitimate forged travel identification documents that are acceptable in seconds (ph).

The analysts at FDL develop hundreds of document alerts. They're sent to border inspectors, have the capability for front-line inspectors to have real-time review of suspect documents and provide forensic investigation support and training.

I encourage all members interested in this issue to travel to Northern Virginia to take a look at the FDL. It's truly a unique resource.

Hopefully during the question and answer period we can talk a little bit about lost and stolen passport issues. We're addressing those through Interpol, through technology development and through our review with the visa-waiver countries -- a critical, critical program to secure those documents.

Terrorism attacks in Asia, Europe and elsewhere are vivid reminders to us that terrorism is an international threat that cannot be conquered alone. We understand we must engage in a global effort each day through collaboration, information-sharing and ongoing dialogue to bring the weight of our collective law enforcement intelligence capabilities to bear against those seek to do us harm.

Thank you for the opportunity to be here. I look forward to your questions.

CAMP:

Thank you very much.

I thank you both for your testimony.

General Hughes, given your extensive experience in intelligence and your understanding of this threat to our homeland, which since 9/11 we've been focused on very intensely, how do you characterize our efforts to track potential terrorists attempting to enter the United States, particularly in comparison to pre-9/11?

HUGHES:

Well, I think it's much improved.

For one thing, the fact that we have standing watch lists as a tool we did not have before, the fact that we have a variety of registration techniques and a much better over-watch on travel documentation, the issuance of passports and visas and certain knowledge provided by the travelers in many cases about who they are and what they intend to do in their travel is a big change. And that does allow us begin to have knowledge of them earlier in the process than we used to.

I think the Department of State may have had that information, but it wasn't integrated into the intelligence and law enforcement and security communities in a way that it is now.

When they reach our borders, of course, as Stewart was discussing here, the US-VISIT program, the enhanced customs and border protection mechanisms at the border when they seek passage into our country, and the knowledge that we have about them combined is a very powerful tool.

And indeed we are, as opposed to tracking them, in many cases we are interdicting them early. We are interdicting them in some cases before they get on an airplane. Occasionally that system fails. When they reach our border generally we know who they are and we are finding them.

I will say that we have some additional capability from the past in illegal border-crossing context. We know quite a lot about activities to our southwest border, Mexico, and some information concerning along the Canadian border -- perhaps a little bit less in the case of Canada because of the construct between our two countries. That's a very powerful tool.

We can in many cases anticipate movement. And we often do interdict persons on those two borders because we knew something about them. We knew they were staging or a group was planning to travel or something like that. It's not perfect, and I don't want to communicate to you that is by any means, but it's better than it used to be.

The last thing I'd like to mention to you is, the term "tracking" is very interesting.

We have not only this foreknowledge, or pre-knowledge, of their activities in many cases, but we are then able to amass this knowledge in a cumulative way, in databases, that did not exist before. This is an invaluable tool and critical to our future success in this regard.

The identification and registration in these databases of these people is vital, and we weren't doing that in the robust way that we are now doing it.

CAMP:

I appreciate that.

I think we all agree that we've been working toward putting together a really strong system in place to apprehend terrorists trying to enter the United States. But it seems to me the more we strengthen our policy at ports of entry, it's also more likely that terrorists may try to infiltrate the country simply by walking across our borders.

Time magazine recently had a fairly chilling article on this issue, and the human smuggling operations and efforts like that.

What is the department doing -- and this may be something the assistant secretary would like to comment on as well -- what is the department doing to strengthen our capabilities to prevent illegal crossings? And how can we use intelligence information to target and detect potential terrorists who may be trying to enter our country in that fashion?

VERDERY:

Well, the short answer is, a lot. And at some point I'd like to follow-on to what General Hughes talked about in terms of overseas efforts, especially on the visa side and US-VISIT.

In terms of the southern border, the enforcement capabilities are growing by leaps and bounds, but it is obviously a very difficult problem.

We have gone this year and in recent years we've increased the number of border patrol agents. We have increased the use of advanced technology, UAVs, sensors, lighting, motion detection and the like. We've put the necessary number of prosecutors and asylum adjudicators and the like on the ground, advanced aircraft deployment.

All this, though, does demonstrate this is a difficult issue with the amount of traffic across the border.

Undersecretary Hutchinson has launched the Arizona border control initiative, ABC, which is really trying to bring operational control to certain sectors in Arizona. It has resulted in huge increases in the number of apprehensions in that sector.

But that, of course, has then put pressure on other sectors. We've had to respond with efforts, such as the Los Angeles Airport initiative, to try to keep people from being moved into LAX and flown to other parts of the country.

We also have to look to our legal authorities, and that's why we've put into place the Expedited Removal Program, to turn around their country nationals quickly who don't have asylum plans, the interior repatriation program to fly Mexicans back into the interior of the country to try to break the cycle of people being just returned across the border.

But over the long haul, we of course need to improve the entire spectrum of apprehension capability, detention capability, removal capability. It's a long-term project that we all have to concentrate on.

HUGHES:

May I just comment on the intelligence piece of this answer, in this open environment?

It's important for me tell you that -- especially with Canada and Mexico, but also with some other countries that are involved, not in crossing the border illegally, as in walking across -- but the illegal border-crossing activity can be facilitated from afar through the use of illegal documentation and false identity. And we do have better and growing cooperation with both Canada and Mexico, and with other countries, in that regard.

Once again, in an open environment, probably wouldn't like to get into the detail, but I can look you directly in the eye and tell you that it's better than it was. It needs to get better than it is, and we are working on that part of this activity.

CAMP:

All right, thank you.

Thank you both very much.

At this time the chair will recognize the ranking member of the Border and Infrastructure Subcommittee, Ms. Sanchez, to inquire.

SANCHEZ:

Thank you, Mr. Chairman.

Thank you, gentlemen, for being before us.

I think the last few weeks in particular the Department of Homeland Security has had some pretty negative press with respect to borders and air -- borders, I think because Time magazine I believe was the one that has that little picture of something being pulled being apart and talked about how much we really do need to do with respect to our borders. And it really didn't highlight the northern border, which of course we all know is much more open than even the southern border.

But I think the other incident that happened was the incident of Yusuf Islam, who everybody in this room probably knows is Cat Stevens.

You guys returned him to England after he arrived in the United States because his name was on a watch list. I think this episode highlights several problems with our current policy, and I sort of want to go through them so I understand what happened.

I think America wants to know what happened and what we're going to do to fix it.

First of all, he was allowed to board the plane. And I guess while he was en route, you guys found his name on a watch list. I guess the question is: Why wouldn't we be checking it before we got a supposed dangerous person on the plane, because maybe he could have blown it up as we were trying to figure out who he was.

So the question is: Why do we have such a huge security gap in the visa waiver program that allows travelers participating in the visa waiver program to get on a plane without first being run through the watch-list check?

And why doesn't DHS check the names of passengers on international flights against terrorist watch lists before the flights take off?

And if you can't do it to all passengers, can you at least do it for the vast majority of passengers who buy international tickets at least an hour in advance?

VERDERY:

I think I'll take that one, Congresswoman.

The Cat Stevens episode does exemplify a current weakness in the way international travelers come to this country.

As you know, we do not have people stationed overseas, except for a couple of selected airports, as I mentioned the immigration security initiative, and essentially the airlines are currently our response overseas to enforce the watch list.

So when a person such as this individual is on a watch list, it is the airlines responsibility to compare the manifest against the watch list and make those no-board determinations. In this case, there was an error made.

We recognize this weakness and have announced, as part of the secure flight initiative for domestic travel, that the international realm will be enhanced by a proposed rule, to be announced later this year, to require that manifest information to be supplied to us in advance of wheels-up, so before the plane takes off.

Now, this will be a very complicated endeavor. It will change the way booking patterns are made, especially for connecting flights from overseas travel, but it would provide much greater security for us to be able to run those watches ourselves through the National Targeting Center before the plane lifts off, and hopefully these tough situations will be much less likely to occur.

You asked about the visa waiver program. Again, the watch list check that is done now is no different whether you're a visa waiver or non-visa waiver. The same error could occur with the airlines enforcing the system.

So that's not the issue in this case. There is a visa-waiver issue we can discuss another time.

We do have the ability -- and this happened during the heightened threat period in the winter -- if there's a plane under a certain threat, we can essentially hold the plane on the Tarmac and run the checks, and that's what was going on. But that is not a tenable solution for all international travel, and that's why we were going to move with this proposed rule to try to get this information ahead of time.

It's also why we went to such great lengths to get the PNR, the backup information about your travel agent, the people you're flying with, and your bags and these kinds of things, frequent flyer number, from the Europeans under this agreement, that we could do that investigative tool both to find people and also to clear people as a potential hit.

SANCHEZ:

You had them for 33 hours, you had his daughter for 33 hours also, because they ended up going off together. After 33 hours you sent him back to England.

In 33 hours you couldn't figure out who this guy was? I mean, it was such a famous person.

I've been trying to figure out what kind of a system are we using to figure out what's going on here.

And did you tell the British authorities?

Why would you put him on a plane if he was such a dangerous person? Did you put him on chained, you know, shackled? I mean, what's the process?

VERDERY:

Well, there's a lot of different issues involved in this situation. There's the "should he have been allowed on the plane issue?" There's the "what should the plane have done while it was in mid-air?" And there's the "how should an individual who actually makes it to our country who's on a no-fly list or a watch list be treated?"

They're all separate issues and all need separate analysis.

But in this case, we feel that he was treated appropriately. He should have not been allowed on the plane, and we had to return him when he arrived in our country after the appropriate booking.

So we need to continue to work on these processes. But we feel that proper procedures were followed once we recognized that he had been allowed to board.

Again, that demonstrates all the more why we need to make these decisions ahead of time, before a person boards the plane.

SANCHEZ:

Thank you, Mr. Chairman.

CAMP:

Thank you very much, thank you.

At this time the chairman of the Intelligence and Counterterrorism Subcommittee, Mr. Gibbons, may inquire.

GIBBONS:

Thank you very much, Mr. Chairman.

General Hughes, again welcome. And I have read your testimony and wanted to ask a series of questions, if I may, because I think it will sort of distill itself down to a point where I think we can get to the heart of the issue here, which is information analysis.

As you stated in your testimony, information analysis is really at the heart, I think, of good intelligence efforts. Absolutely, if you don't have good analysis, no matter how good the collection is, the result is going to be flawed.

So my question is: When you have several other departments, or components within the department of homeland defense, that maintain distinct intelligence units, what kind of control do you have, as the head of the information analysis, over these other intelligence offices?

Is there a need for a structured relationship between IA and these offices? If there isn't one, should there be one?

And tasking, describe for me the tasking ability of IA to these other offices in order that you get the right information to make a decision from your standpoint.

HUGHES:

The answer, sir, I think is -- I'll start from the back and go forward here.

The capabilities resident in all of the organizations that I enumerated in my formal statement are impressive. They all produce what I call organizational intelligence. They're focused on their organizations.

The Secret Service, as an example, is exclusively focused on missions and matters at hand for the Secret Service. And they're very closely held and are not broadly applied, for a very good reason.

Conversely, perhaps the United States Coast Guard, a member of the U.S. intelligence community in its own right, it's a bona fide member -- it has its own budgetary line and its own identity -- has a very broad set of capabilities akin to any other armed force.

And I'll just describe one more example: Immigration and Customs Enforcement, which in large measure operates in a clandestine manner and is a very capable organization in the human intelligence context.

All of those, and others that I want to take the time to enumerate, together, taken together, find their way into the national intelligence community through their own conduit and through the Department of Homeland Security. It depends on the circumstances, the nature of the reporting.

But virtually everything of departmental and national interest comes to us at some point.

I believe we have value-added in regard to the analysis of all of that information. We're able to put it together, assemble it in one place, cause it to become synergistic in nature.

The answer to the last part of your question, sir: We can task anyone inside the Department of Homeland Security in the name of the secretary, and we do.

GIBBONS:

Is there a structured relationship between you and these other intelligence agencies?

HUGHES:

Yes, there is.

We have an agreement among us, which has been verified by the secretary and by their individual organizational leaders, that IA is the departmental organization that gives some form to the structure. We meet every two weeks formally in the Homeland Security intelligence group context, and we exchange information among us and between us.

We also have call participation in many meetings, and interaction every day exists between us in automated form, by telephone, and in many cases face-to-face meetings that occur because we interact.

VERDERY:

Congressman, if I could just add to this from the BTS perspective...

GIBBONS:

Yes.

VERDERY:

... and that's one of the points of having the Border and Transportation Security Directorate as an umbrella over these large operational components -- CBP, ICE, TSA. They have their own headquarters. They're operating around the country, around the world.

BTS is at headquarters with IA, so there's constant interaction between General Hughes' operation and the BTS headquarters operation at the NAC, and also to coordinate -- we recognize that the activities, intelligence or otherwise, between the BTS components are so linked, especially between ICE and CBP, because essentially Congress broke INS and Customs in half and put the investigators with the investigators, and the inspectors are the inspectors, but those links between the two, to bring front-line activity back to the investigative realm has to be maintained, and that's one of the large purposes of the BTS directorate, is to make sure that link continues along with the agency intelligence from headquarters out to the field.

GIBBONS:

Well, Secretary Verdery, let me ask this: You just talked about having 838 apparent hits on your watch list, with one- third receiving some sort of adverse action, either arrested or rejected for entry due to the biometrics program that you've got.

What are you doing today to enhance the current capability of biometrics? In other words, are you looking at new technologies that are out there so that we don't get, as Ms. Sanchez, said an inadvertent hit because of the inability either to not have the information that was properly there or to have a poor biometric system that doesn't do what we expect it to do?

What programs, what pilot efforts have you got going, what research and development? Are you reaching out to the private sector to do this?

VERDERY:

Well, sir, the VISIT system, which you referenced, is obviously a fingerprint, finger-scan-based system.

Secretary Ridge, the attorney general, the secretary of state made a decision to base it on fingerprints largely because that's how we have people listed in criminal databases and also on terrorist watch lists in many cases by the fingerprints. That's what makes us able to find people.

It's worked extremely well. I think the turnaround time is running about six seconds from a systems perspective...

(CROSSTALK)

GIBBONS:

There are also other systems out there that could be supplemented to the fingerprint system that could be very helpful.

VERDERY:

There are. And VISIT is always looking at trying to find repetitive or back-up systems that would enhance the biometrics, the facial recognition part of the biometric passport, which will be coming online throughout next year, will be part of the VISIT system. We have to deploy readers to read those biometrics, facial recognitions part to the passport, and build that into the database.

We're looking at other biometrics, whether it's iris or the like, and that can be built in on top of that.

Now, it's a very important thing, the president issued HSPD-11, Homeland Security Presidential Directive 11, last month, which requires our department to go through a screening review of all things across the government, including biometric screening processes, to harmonize them, to come up with the best biometrics, the best screening procedures to make them consistent. That review is ongoing right now with a biometric subgroup.

The other thing I should mention, our Science and Technology Directorate, not represented here, is putting in an incredible amount of effort to next-generation biometrics, working with our operational entities like US-VISIT.

GIBBONS:

Well, at some point I'd like to talk to you personally about these systems, and I look forward to that.

Thank you, Mr. Chairman.

CAMP:

Thank you.

At this time the chair recognizes the ranking member of the Intelligence and Counterterrorism Subcommittee, Ms. McCarthy, to inquire.

MCCARTHY:

Thank you, Mr. Chairman.

I have a question for each one of you, but I'll take Mr. Verdery first.

I appreciate that you said that we're not under the practice of holding planes when we are checking watch lists. I happen to agree with you on that.

But in a journey I made during the recess period, I read that Australia has a system now where they do that investigation when the individual buys the ticket. And I wonder if we're moving in that direction. There's legislation in the House, sponsored by our ranking member, to encourage that.

Would you give us your thoughts?

VERDERY:

Yes, ma'am.

As I mentioned, we have announced that we are planning to promulgate a draft rule that requires that advanced manifest information to be supplied before the plane takes off so we could do the vetting at the National Targeting Center before the planes gets into the air.

So that's something that will be coming down the pike.

Now, I will say, to be candid, it is not an easy solution. Because if you talk to airports, airlines, the way that the changes that will have to be made to how people are booked twice, the way people connect on flights, will be immense.

There will be costs here, both in terms of inconvenience to passengers, the way airports are structured and the like.

We support it. We think it's the right way to go, but it is something that has to be managed very carefully to make sure we don't kill off the travel industry in the process.

MCCARTHY:

Well, it hasn't killed off the travel industry in Australia, so I think there's probably a good model for you out there.

People who are bargain shopping are generally buying their tickets ahead of time, and that should be of assistance in your efforts as well.

I think it's only members of Congress that don't know when they're getting on a plane.

VERDERY:

It is of assistance, but of course when you're talking about millions of incoming travelers, even if you have a 1 percent error rate, where you're talking to the travel agent on the phone and you say your name or an address or a phone number and they mistype a key or a number, that then ends up with the kind of false hit that you try to avoid.

So that's why the system right now is based on the information on your passport that is swiped electronically at the desk, at the check- in counter, so there aren't errors, very rarely, in that kind of information taking.

You take it off the phone, off the Internet, you end up with more errors.

MCCARTHY:

Well, I have every faith that you'll figure this out and we'll do an even better job than Australia.

General, does DHS or TTIC or any of the other intelligence agencies have an office devoted specifically to terrorist travel?

The information-sharing that is going on in other countries, I was on a trip with Member Dunn, who chaired the trip to Ireland, to Northern Ireland, the Republic of Ireland and England, and one of the examples we learned there was that a police officer in Northern Ireland investigating an incident uncovered information that when shared with others in the Republic of Ireland, in the south, and with Great Britain, led to the discovery of the cell that funded the Bali tragedy and others.

Albeit they're all in one compact series of islands, are doing that information-sharing.

How are doing on information-sharing, not just within our own country but within those other strategic countries that are so important to our mutual success?

HUGHES:

Well, it's a good question but it's broader than the Department of Homeland Security. I'll go ahead and answer it on behalf of many other colleagues.

The U.S. intelligence community, at a variety of levels, especially the Central Intelligence Agency, the Department of State's intelligence organs, the Federal Bureau of Investigation, and the Defense Intelligence Agency and the Department of Homeland Security, we all exchange information with other countries.

It's not perfect in some cases. And the reasons are, we have to go forward with information that can be released and placed at risk in the other countries' realm.

We do have mechanisms to do that, such as terror lines of sanitization where you take out the source's methods that we used to get the information.

It's a very robust activity, and ongoing.

I think it was kind of an interior question there that you asked, and that is, how are we doing with regard to the terrorist travel focus.

The Transportation Security Administration's intelligence organisms -- there are two or three different pieces to that -- do over-watch terrorist travel in a professional sense. And in my organization, as part of our strategic intelligence division, we have a combination of liaison officers and devoted analysts who work part- time or whole-time on the issue of terrorist travel.

Indeed, I would probably say each and everyday my time is devoted in some measure to the issue of persons who we have encountered in the travel process who are connected in some way with terrorism.

It's of vital importance to us.

MCCARTHY:

Mr. Chairman, may I pursue very, very briefly?

CAMP:

Very briefly, the gentlewoman's time has expired.

MCCARTHY:

Yes, sir.

Is there a clear sharing with other countries?

HUGHES:

Yes.

MCCARTHY:

Thank you.

CAMP:

The gentleman from New Jersey, Mr. Andrews, may inquire.

ANDREWS:

Thank you, Mr. Chairman. I appreciate the testimony of the witnesses.

Our goal, our policy is to reach a day when every person attempting to gain entry into the country can be affirmatively identified so we know who they say they are.

When will we reach the day where every port of entry into the country has biometric reading capability?

VERDERY:

We've already deployed some of (ph) US-VISIT biometric reading capability. That's been deployed to the major seaports. There are some smaller ones that have not been brought online. That will be coming down the pike throughout the coming months and years.

In addition to that gap, we're deploying it at the land borders, at the 50 largest land borders, at the end of this year and the smaller ports of entry throughout next year.

US-VISIT is not a complete system by any means. But the secretary I think took the bold step of deploying it in stages.

No one's been able to do this because no one -- was going to kind of do it in parts.

ANDREWS:

I understand. You want to do it right rather than fast, but we want to do it right and fast.

So what percentage of people coming into the country today do not have their IDs biometrically read?

VERDERY:

Well, I'm trying to remember. The overwhelming number of people who come into this country are coming via the land border, and the larger percentage of that is from Mexico.

Now, most people coming in from Mexico are border-crossing car- holders. I'd have to get the numbers for you.

But my sense of it is at least probably a third of individuals coming in are coming in as border-crossing car-holders, you know, coming back and forth all time.

Those people have gone through a background check, (inaudible) to a visa, so they've been checked.

Anybody who's going through (ph) a visa has been checked.

And now, starting today...

ANDREWS:

When you say checked, you mean read through a biometric reading?

VERDERY:

Anybody who goes -- you apply for a visa now, you will go through a biometric check at the time of the visa interview, and then again with US-VISIT at the port of entry to see if derogatory information has been received in the meantime or if you've forged your document.

And, again, as of today, literally today, visa-waiver travelers who don't have the visa are now being checked biometrically at the port of entry, at the airports and seaports.

ANDREWS:

I know that it's not a totally knowable fact to know when the day will come when every port of entry has biometric reading capability, but when do you think the day will come?

VERDERY:

I think we are aiming -- the most difficult will be the smallest land ports of entry, which is by statute required by the end of 2005. These are the outposts in the middle of nowhere, so to speak.

So that's the backdrop of the last date where things would be fully...

ANDREWS:

Is that going to happen?

VERDERY:

I believe it will, yes.

We are committed to have the big ports of entry with that capability in secondary at the end of this year, building out into primary lanes of entry throughout next year.

ANDREWS:

This will include by sea, by air, by land.

VERDERY:

Air is complete right now for entry, and the seaports largely complete, there are a few gaps. Land, this year and next.

ANDREWS:

Now, let's talk a bit about biometric quality.

Dr. Wein is going to testify later this afternoon. He's concluded that a very, very small number of the readings are reliable, and he's made a suggestion that if we shift the technology for the fingerprint reading to read 10 fingers, instead of what we read now, we could dramatically increase reliability I believe over 90 percent from in the 40s or 50s where it is now.

A, do you agree with his assessment?

And, B, if you don't, what's wrong with this assessment? And if you do agree with his assessment, do you think that we should make the rather modest technological change that he's proposed to try to plug the hole?

VERDERY:

All I've seen is his testimony for this hearing, which doesn't have the technical backup that you might expect. I understand he has a study that will be released in the coming days, which I would expect that our team, especially the US-VISIT office, would want to look at very carefully.

As I understand it, it's not that the majority are unreliable; it's that a small minority are unreliable if they have certain characteristics of their fingerprint, which I honestly feel a little uncomfortable talking about in open session as to how the visa system, to be honest.

ANDREW:

But certainly we could generically say that there are people trying to beat the system and there are ways to do it. Right?

So do you agree with his conclusion that those of significant plurality, I guess, of those who try to beat the system can do so now?

VERDERY:

I don't agree with that, and I don't believe our US- VISIT biometric experts do either. I don't pretend to be a biometric expert, but I don't believe they agree with that in the way it's been presented.

Now, to go to the question you asked earlier about the 10-print: I think we do agree that in a perfect world a 10-print solution, if it didn't take any more time and any more cost, would be preferable. But at a port of entry, at a visa-issuance window, there is a big difference between putting a 10-print reader and a two-print reader out in a primary lane at a very private consular office.

So the marginal gain between 10-print and two-print we have decided to date is not worth it because it would have held up deployment of a system that is working every day, as we speak, to find people you would not coming into this country.

ANDREWS:

Actually, I'm concerned about that answer, because it's my understanding that NIST looked at this study and believes that the professor's conclusions were conservative, that in fact that the error rate may be higher.

And remember that although the vast majority of people trying to get entrance do not in any way try to alter their fingerprint. I would assume that it's a pretty fair conclusion that a significant number of people are actively trying to keep out...

(CROSSTALK)

ANDREWS:

So it's a small part of the universe, but a very crucial part of the universe.

Let me also ask you this, and it follows up on Mr. Gibbons' question: What mechanism is in place to move forward in biometric technology for things other than fingerprints, like eye scan? Do we have the flexibility to test those technologies? And if so, what are we doing?

VERDERY:

Well, we're actually testing the iris scan, if that's what you mean, right now in a different program, the Registered Traveler Program that TSA is operating at five airports around the country, including Reagan National, both fingerprints and iris scans as a way to verify people who've been pre-enrolled in a Registered Traveler Program.

So we are working on the iris from that end.

As I mentioned, the facial recognition technology that will be built into international passports that will be required of visa- wavier travelers, next year we are building in a capability to read that into our document readers at ports of entry.

So we're looking at the systems that provide redundancy and the like.

But, again, the backbone of the system from all points of view has to be the fingerprints, because that's the way that our criminal records are characterized, that's how we're able to find people very quickly with very low error rates, people who should not be admitted to this country.

ANDREWS:

Thank you very much.

CAMP:

Thank you.

Mr. Pascrell may inquire.

PASCRELL:

Thank you, Mr. Chairman.

Mr. Chairman, 98 percent of over 281 million visitors annually enter our country. That means that millions of travelers entering the country are entering without being checked against any intelligence database that could help identify a potential terrorist or even a convicted criminal.

I'm interested when we talk about terror, General, I want to know if you agree with me.

I am talking not only about those people who wish to bring explosives into this country, or to come into this country to wreak havoc on our citizens and our property. I'm talking about those people who are transporting drugs across our border. I see that terror everyday in my district, throughout this nation.

And I know that drug trafficking in the United States has a lot to do with the funding and in assisting of terrorist groups and organizations.

What do you see and what do you do about drug interdiction? And how do you see they're both connected?

HUGHES:

Well, thank you very much for the question.

Perhaps Assistant Secretary Verdery would like to comment after I do.

First, I'm not positive about the figures you quoted. But I grant you that there are people who successfully get into the country with drugs and who are terrorists who may come in with some capability. That certainly is true.

I think it's a very small percentage compared to what it was.

We have actually been extremely successful in interdicting drug shipments. And indeed, in the past two weeks, we've interdicted a huge multi-ton, ship-borne movements of cocaine in the Pacific, which you may have read about in the newspapers.

Aside from that, on our land borders and in air crossings, it's a pretty common for us to now interdict any kind of carrying such material, either terrorist-related material or drug materials, through the air bridge.

The land bridge, as we've mentioned, poses a significant problem for us. We're trying to do our best to control that, and there are a lot of issues there I could talk to you about.

But I think we are making progress. We're on the right track.

I don't know if that's a good answer for you, but I'll summarize it: Maritime is a huge problem, but we are being successful with interdicting, and that's often based on good intelligence.

The air bridge is pretty secure, comparatively, for both terrorist activity involving materiel and for narcotics trafficking. Small amounts probably arrive here and there.

The land borders are an issue, and we're working hard to secure them.

PASCRELL:

Mr. Verdery, would you respond to that question?

VERDERY:

Sure.

I think, as General Hughes, that the numbers on drug seizures are up quite dramatically, whether it's by sea with the Coast Guard or over land at our ports of entry or the border patrol.

We've seen a no-degradation of the drug mission in this department. In fact, it's been enhanced by the additional capabilities being brought to bear.

I'd be happy to get you those figures on that.

We do recognize, of course, that the means by which people are able to enter the country on the land border could facilitate a terrorist looking for the same type of entry. That makes it all the more important...

PASCRELL:

My point -- excuse me for interrupting -- my point is that there is no difference in the terrorists. What's the difference?

If you're bringing drugs into this country to kill our children and our citizens who are stupid enough to use it, what's the difference between that kind of terrorism and the terrorism that the president's been talking about over the last three years? What is the difference?

VERDERY:

I take the point.

We want to do both. We want to fight -- counternarcotics mission and also what I was referring to is more of international terrorism, which I think is a term of art...

PASCRELL:

Well, would you agree with my statement that the terror of drugs in this country is just as horrible, just as terrible as the terror which is brought into this country of those who wish to bring explosives or to kill our citizens or to damage our property?

VERDERY:

I wouldn't want to rank two horrible outcomes. They're both horrific.

PASCRELL:

We both agree, then?

VERDERY:

Yes.

As I was saying, I think the capabilities that are being brought to bear against the terrorism threat -- as I define it as international terrorism, Al Qaida and the like -- is having significant impact on the drug enforcement mission also, whether it's the "One Face at the Border Initiative," getting our customs inspectors and immigration inspectors cross-trained, enhanced border patrol missions, advanced technology on the border.

We are seeing increases in picking up people, picking up drugs -- all those kinds of things on the border.

The last point I have to make is that this demonstrates all the more the reason for the president's guest worker initiative.

Because we've got to figure out a way to get the overwhelming majority of people who are crossing the border illegally, who are not criminals, who are not trafficking in drugs, who are not terrorists, who want to work, we have to be able to have them a way to come back and forth to those jobs through the ports of entry where they can be vetted for security reasons and essentially pull the wheat and the chaff, separate them.

Terrorists are not going to be able to walk into a port of entry. So if we can get the guest workers through there to work, coming back and forth, report to (inaudible), regularize that, it would make our border enforcement mission much better.

PASCRELL:

I didn't make myself clear, then.

There are 22,000 Americans who are killed every year in the United States due to illicit drugs. It would seem to me -- just an observation, a perception -- that we do not have the commitment to interdicting those drugs and ending this horror on the streets of our communities.

Now, we know the tragedy of 9/11. The commission spelled it out, made some recommendations. Some we've included in legislation conveniently, and some we've left out

You don't have enough to do your job. I don't care what you tell us today. You don't have enough people to do your job.

So you're the messenger. I understand that. It's not you personally that I'm...

VERDERY:

There is a commitment from the department, from the secretary, from Asa Hutchinson, the undersecretary, former head of the DEA, our deputy secretary, our operational head, Commissioner Bonner and the like in our counternarcotics office to see this mission forward.

And as General Hughes mentioned, the numbers bear out that we are doing it.

Are drugs getting in? Of course. This is never 100 percent solution.

But we have seen a robust increase in the amount of drugs that are interdicted in the source zone, at the ports of entry and the like. We need to ramp it up, but we're doing the job.

PASCRELL:

I just wanted to bring something to your attention, and that is: In the border patrol, we're talking about -- in 2001 there were 9,700, almost 9,800, border patrol. There's 10,839 today.

How can you sit there and tell this committee, being the messengers, how can you sit there and tell this committee that by adding this small amount of border patrol that you are even touching the surface of this serious problem?

You know that there's more drugs coming into this country than ever in the history of the nation. You don't have enough people to do the job.

We're doing this on the cheap, and we're being -- for what reasons? I don't know why we're holding this hearing today, I really don't.

We need to act, and we need to act yesterday. That was the whole message of the 9/11 commission. We need to act yesterday. And we need to do it in a very tangible way rather than simply having committee upon committee, everybody gets a piece of this, and nothing is being done.

There's terror in our streets and there's terror from drugs in this country that are moving freely. You know it and I know it -- just as serious as the lunatics that are out to try to kill us. Just as serious.

CAMP:

Thank you. The gentleman's time is expired.

Before I recognize Ms. Lowey, the purpose of this hearing is to look at terrorist travel. We have separate committees in this House to deal with narcotics, and there are some members that are on both committees, like Mr. Souder, Chairman Souder, who's done a great deal of work in this area.

So I appreciate the gentleman's line of questioning, but this hearing, in fairness to our witnesses, is about terrorist travel. And I realize...

PASCRELL:

We're talking about terrorist travel, Mr. Chairman.

CAMP:

I realize by your definition, but we have separate committees...

PASCRELL:

That's why I asked the question.

CAMP:

Yes, but we have separate areas that are also working on this.

So with that I would recognize the gentlewoman from New York, Ms. Lowey, to inquire.

LOWEY:

Thank you, Mr. Chairman.

Gentlemen, good to see you again.

Tuesday's New York Times reported, based on the findings of an FBI inspector general report, that three years after September 11th attacks, more than 120,000 hours of potentially valuable terrorism- related recordings have not yet been translated by linguists at the FBI.

My judgment: This is absolutely outrageous, not to mention dangerous, particularly for the residents of my home state of New York, which is referenced in an intelligent reports time and time again.

In my judgment we can collect all the intelligence we want, but if we let it set on a shelf and collect dust for three years, it won't do us any good.

We're here today in part to review the progress being made by the department in the area of information-sharing.

Perhaps, Secretary Hughes, could you just tell me what this report indicates to you and what you're doing about it?

HUGHES:

It indicates to me that we -- and actually I guess I'll use a little bit of history here -- we haven't solved the problem we've had for many years. Similar kinds of records have been found throughout the intelligence community, not just at the FBI, but at the National Security Agency, Central Intelligence Agency and the former office that I held, the Defense Intelligence Agency.

We are overwhelmed, in fact, many times by the volume of material.

We do have some screening mechanisms to go through this material and highlight to us the issues of interest that are in them rapidly. Key word search as an example of anything that can be digitized. That's not the only...

LOWEY:

Secretary Hughes, if I may, but I know my time is fast disappearing.

You are the assistant secretary, information and analysis.

HUGHES:

Indeed.

LOWEY:

And I may not get to my question about border security.

But it's three years after 9/11. I have three children, I have seven grandchildren. I want to know what you or others who have similar responsibilities are doing about this now.

This is an embarrassment. It should be an embarrassment to you, to Secretary Ridge, to the FBI. What are we doing about it now?

HUGHES:

I don't think I can answer your question. I don't know what we're doing about it now outside of being equally outraged, as you are, about the report.

I don't actually know if the report is completely accurate. But let's assume that it is for a minute.

What I intend to do is to ask questions about it in the appropriate forum and to seek full detail and then search for ways to solve this problem.

I'm sorry if I seem like I was talking on about something that wasn't related. But indeed it is related, ma'am. We have had these problems for 20 years or more. And we are likely to have them in the future.

The volume of information and the number of people to deal with it is in great imbalance.

I apologize for giving you that answer.

LOWEY:

No, I appreciate your honesty, sir.

But I just want to say, as someone who sits Appropriations, in addition to this committee, I know the billions that we're spending.

We spent billions organizing this Department of Homeland Security. I have real concerns that instead of dealing with issues like this and replacing incompetent people with competent people -- we've been moving chairs around. Some people aren't even in their offices yet.

So I just wanted to send a very strong message that if my first responders -- my police, my fire fighters -- are going to be getting plans in place to deal with emergencies -- and the FBI doesn't even have all the urgent messages interpreted.

As you know, before 9/11, part of the problem was they couldn't get the messages to the right people. And I'm not even talking about other issues that our first responders have.

But if we can't get these messages interpreted in a timely way, we might as well all just say: Give up, save the money, put it into our schools, put it into our health care. The Department of Homeland Security is just not doing what it should.

I hate to be so strong because I know you're working so hard.

But I just hope that if I'm sending my strong message to you, it's gotten, and you can report back to me and to the committee as soon as possible with a plan that is going to address this.

I don't know if we're going to have -- in eight seconds -- I don't know if we're going to have a chance to ask other questions.

But Solomon Ortiz, my colleague, has been asking a lot of questions about the gangs, the illegal immigrants that have been coming over the border. Unfortunately, the head of counterterrorism at the CIA never heard about that.

So I hope, Mr. Chairman, I hope you all have heard about it.

He didn't know about it.

So there seems to be a real problem of people in one office not communicating with people in other offices.

I hope, Mr. Chairman, if we have another round, we can deal with that, because that is truly a major issue on border security.

Thank you.

HUGHES:

I have just one brief answer to this last question.

LOWEY:

I'm talking about the catch-and-release issue.

HUGHES:

I understand and the gangs issue.

My point I was going to make is: One of our primary databases is called VGTOF. It is the violent gangs and terrorist organizations database.

We combined the two in at least one database and look at them with equal vigor for lots of reasons. And part of the reason is, we believe, I strongly believe, there is a connection.

So MS-13 from El Salvador or Honduras here in the United States and Al Qaida somewhere else I believe does have a relationship that's important for us to understand.

May I just close by saying: I share your passion, and I'll do my best, ma'am.

CAMP:

Thank you.

LOWEY:

Mr. Chairman, I think it's just important to remember -- and I know if we get to another round -- that the problem here is that these illegal immigrants are released under their own recognizance. And I have a feeling they might not all be home just knitting with their families or cooking dinner.

I think it's an amazing issue that many of my colleagues have spent a lot more time focusing on, and I was just going to bring it up today.

Thank you, Mr. Chairman.

CAMP:

Mr. Langevin may inquire.

VERDERY:

If I could just have just a brief minute to respond.

CAMP:

Very briefly.

VERDERY:

I'll try to give it very quick.

But you mentioned the words catch and release, and that's obviously a concern of ours.

There is an imbalance between the number of people who are picked up who are scheduled for deportation and the amount of beds we have.

Now, within that imbalance, ICE has gone to great lengths to prioritize people who have been found to be involved with criminal activity, violent criminal activity, or non-Mexican.

So we are trying to prioritize amongst our bed space to keep the violent felons, these folks, in custody until they're deported, as well as trying to improve the deportation system itself to get more people through the system, whether it's through repatriation, getting people back to countries that won't take them.

We're trying to move more people through so we have less catch and release.

CAMP:

Thank you.

LOWEY:

Maybe you should have more bed space.

But, Mr. Chairman, I won't take anymore time.

CAMP:

Thank you.

Mr. Langevin may inquire.

LANGEVIN:

Thank you, Mr. Chairman.

Gentlemen, thank you for being here today.

Myself and Mr. Andrews are clearly on the same wave length, and he addressed my question in a large part.

But I do want to follow on, if I could, and explore just a little further where we are, how close we are in terms of having a robust system that is as close as possible to 100 percent effective when it comes biometric scanning of fingerprints.

What are you doing to get us to that 100 percent level?

In terms of a time frame, at what point can you give assurance to the public that we are as close as we're going to get that it is a 100 percent accurate scanning system.

In addition to that: Are we giving equal attention, in terms of the technology that's deployed, to airports, ports of entry and land border crossing, particularly in light of the fact that there is some suggested Al Qaida would prefer a port of entry as opposed to some of the other methods, coming in.

VERDERY:

Well, thank you for the question, sir.

Again, VISIT is being deployed in fairly well identified discreet increments.

Increment one, January 5, this year, airports and seaports, is now 100 percent at airports. So every international traveler, with the exception of, like, diplomats and a couple of other minor things, basically 100 percent are vetted biometrically at the port of entry at airports.

Seaports is close to 100 percent for entry.

Land borders: We'll put US-VISIT capabilities in secondary processing by the end of this year at the 50 biggest ports, the very heavily trafficked ones, and at the smaller ports of entry will end up next year, by 12/31/05.

The VISIT capability on primary -- this is essentially when your cars are driving through on primary -- will be deployed through 2005 at the big ports of entry, in 2006 for small ports of entry.

In terms of how are we deploying it: We recognize there's no way to make everyone get out of a car at primary with literally millions of people coming through. So we are going to be going with a radio-frequency technology solution so that the biometric information is pulled off your travel document as you're going through the port of entry ahead of time so the inspector can see the information, see if there's a potential problem, while there's still time for a law enforcement response or other necessary action. And then the same solution will be deployed on exit, so there's an exit at the port of entry as well for land.

I think I mentioned the airport exit solutions -- maybe I haven't -- but that will be deployed, pilot this year, and throughout next year, there'll be a universal airport exit, seaport exit.

So I think the bottom line for airports and seaports, you're looking at near 100 percent coverage by the end of next year; land ports, 2006.

LANGEVIN:

What about the accuracy of the technology itself? Mr. Andrews brought up, Professor Wein's findings indicate that the technology itself in some cases may be as low as 52 or 53 percent in terms of its accuracy. You feel it's higher. But clearly it's not at 100 percent.

So what steps are taking to get it as close to 100 percent accuracy as possible? And how long before you have confidence that it is 100 percent accurate when the technology is used?

VERDERY:

Well, what we found in these 9 million or so people who've been enrolled in US-VISIT this year is that the accuracy is quite high. The false positive rate is less than 1 percent, and those people are resolved usually very quickly, in a couple of minutes, in secondary where a fingerprint appears to be a match against a watch list but is not.

There are small numbers of individuals whose fingerprints cannot be taken for medical reasons or other reasons.

The issue that's raised by the witness in the second panel is I think a little bit different than that. It's a question of, if you're trying defeat it, how easy is it to essentially try to rig the system.

Again, I don't feel we're comfortable talking about that in open session. I'd be happy to come in and talk to you privately about that.

But in terms of the overriding majority of individuals, it's working extremely well, in the 99 percent range.

LANGEVIN:

My time is almost up, so quickly I'd like to ask: I still am constantly baffled by the sheer number of different databases and lists available for determining who requires extra screening and who should or should not be flying.

And I can't believe that we still don't have one complete integrated list that can be effectively used for our transportation and border security infrastructure to thwart terrorist travel.

So can you provide some more details as to what your goal is in terms of streamlining those lists and ensuring that they are used effectively? And can you tell me exactly when that goal will be met?

VERDERY:

Well, the watch-listing effort is led by the Terrorist Screening Center, established by the president I believe last year. That responsibility is being handled now. The terrorist screening database is what is accessed by our front-line people, whether it's a TSA screener or an airline in terms of enforcing the no-fly list.

So essentially we do have a common set of watch lists that are now used, depending on the program.

So the problem we have, and the reason you see these stories in the paper of people being flagged in appropriately and the like, is not so much a problem with the list; it's a problem with the implementation of the list.

Right now it's being run by each of 77 airlines differently. Essentially your person that's checking you in is essentially acting as the watch-list enforcement person.

But we recognize that's not a tenable solution. That's why we've proposed a secure flight program to bring that responsibility within the government's sphere, within the TSA, Transportation Security Administration.

But to do that, we have to get the information from the passenger, via the airlines, in time to make that determination. So we've issued an order to compel data for testing of the system. That will be followed on by an order compelling data to make this (inaudible) so that we can handle this and not put the airlines in the responsibility of trying to enforce these lists.

But it will be based on the Terrorist Screening Center's coordinated watch list.

LANGEVIN:

Can you give a time frame? Can you assure the public out there that we're not going to see these kinds of stories in the paper where we've got different lists that don't pick up accurately people that should not be flying?

VERDERY:

Secure Flight I believe is due to become operational in the spring, post-testing. That's when you'll see the transition from the airline-based system to the government-based system.

Will it be 100 percent? No. Because there are so many air travelers, there will be false hits. If we have somebody on a watch list whose name is Bill Jones, there will be other people named Bill Jones who are flying, and we have to resolve those types of potential hits.

I'm always amazed at how many similar names there are, even when they don't sound like a common name. But you put the entire American people and the international travelers out there flying, you're going to have those types of hits that have to be resolved, and that's why we're working on Secure Flight.

CAMP:

Thank you.

The ranking member of the full committee, Mr. Turner, is recognized, if he would like to inquire.

TURNER:

Thank you, Mr. Chairman.

I think the first thing I'd like to talk about is this problem we have on the border with the catch-and-release practice that's ongoing.

Do we have a figure available, Secretary Verdery, that would tell us what it would cost us to end that practice?

VERDERY:

A figure on how much it would cost to detain every person whose apprehended until they're deported?

TURNER:

Yes.

VERDERY:

I do not have that in front of me. It would be quite large.

TURNER:

Has there been any consideration of some temporary detention facilities that would enable us to halt that practice?

VERDERY:

Well, there are temporary facilities used on occasion. That's what we've done in Arizona, where we've gone in and enhanced the resources.

We recognize there has to always be a balance of the prosecutorial resources, the detention sources, the removal resources. If you end up with an imbalance, you essentially haven't done any good because you can't get people through the system appropriately. So it has to essentially a continuum.

So in that case, we have put more temporary space in Arizona.

TURNER:

I'm told by some of the border patrol people that I've visited with that the catch-and-release practice fairly quickly has become well known among those who are engaged in human smuggling.

And so we are likely to have seen an increase in efforts to come across our unprotected borders as a result of the fact that it has become known that if you're from a place other than Mexico, you have about a 50 percent chance of being released on your personal bond if you come into our country.

I would suspect that we could at least make some impact upon the movement of illegal immigrants from places other than Mexico if we made some effort to try to stop that practice.

VERDERY:

Well, that makes the announcement we had recently of the new use of expediter removal points up the need for that. It essentially is going to say, "If you're from a country other than Mexico and picked up between a port of entry, not having asylum claim, you're going to be held, whether it's a couple of days, in a short period of time you're going to be flown back. You're not going to put into the system, taking up a bed for months, even years." We can move people through more quickly.

Again, I've got to get our numbers, but the detention numbers -- 108,000 in '01; 113,000 in '02; 145,000 in '03; we had 130,000 in '04 through June.

So I think we're on track to have quite a bit of increase from last year.

But, again, there is no shortage of people in this regard.

TURNER:

The border patrol people that I visited with say that they have received no instruction from the department regarding how this new expedited deportation process is going to work, no indication of what kind of training the border patrol agents will be receiving, no indication of when this is going to be implemented.

We have a program here that you have announced, but there doesn't seem to be much understanding among the rank and file about how it's going to work or where you're getting the money to pay for it.

Could you help enlighten us on that?

VERDERY:

Well, it's operational in two sectors, in Tucson in Arizona and Laredo in Texas. So if you're not a border patrol agent in those two sectors, then you probably wouldn't have been trained because it's not being applied.

And those sectors' training has been completed. I'd have to get back to you on exactly how many people, but the training has been provided. There was a month lag time between the announcement and when it

became operational so they get their proper training to make sure we're abiding by our asylum requirements under international law.

In terms of the funding, this is a money-saver over the long haul. It's going to move more people through and will be a deterrent effect against the migrant flow that you've mention.

If I might just mention one other thing while I have the floor, a very important announcement from last week, is we've now integrated at the border patrol stations the IDENT and IAFIS fingerprint systems, which were formerly separate systems developed by the Justice Department.

They're now fully -- have integrated workstations available at all border patrol stations, so if the border patrol picks somebody up, they can not only check against IDENT, which has information about prior illegal crossings and immigration information, but also against IAFIS, which has all the criminal database from FBI and other sources.

So we'll have an end to that situation where people were picked up for a crime in one state and then border patrol didn't know about.

So we've already had a number of successes of violent criminals being found. Of course, that means those are the types of people we are going to detain. They're not going to be catch-and-release policy, so to speak. And those are the priority people that will take up those beds.

TURNER:

Do you have the capability to access the FBI database to know who they may have on their database when people come to border patrol stations?

VERDERY:

Well, that's in fact what I was just talking about, the IAFIS system is what FBI operates.

So, yes, if border patrol picks somebody up, they are now run against IAFIS to see if there's a prior criminal record. That is now -- we had promised that it was going to be deployed in 70 percent of the border patrol stations by the end of this year, and we've beaten that by going to 100 percent as of last week.

TURNER:

And do you feed information back to the FBI regarding people that you pick up, or that your records -- you feed into that same database just as you receive information from it?

VERDERY:

They have access to IDENT through the US-VISIT program. And we've actually just announced an enhanced access by FBI to do searching through IDENT, whether it's the border patrol information you mentioned or the entry-exit information through US-VISIT. They do have access to that and we're enhancing that.

CAMP:

Thank you. The gentleman's time has expired.

We have another panelist that we'd like to hear from.

I want to thank both General Hughes and Assistant Secretary Verdery for being here this afternoon.

This will conclude your testimony before this subcommittee today. Thanks again for being here.

VERDERY:

Thank you.

CAMP:

The next panel will include Professor Wein.

I want to thank Professor Wein for coming all the way from the California to testify at this hearing.

Professor Wein can come and take a seat at the table.

Thank you. We have your written testimony -- if you could briefly summarize your statement in five minutes.

WEIN:

Good afternoon, Chairmen Camp and Gibbons, Ranking Member Turner and the members of the House Select Committee on Homeland Security.

I'm honored to appear before you today to discuss the serious but reparable vulnerability in the biometric identification performance of the US-VISIT program.

The implications of our findings are disturbing enough that last week I briefed members of the Homeland Security Committee staff from the Office of the Vice President, analysts at General Accounting Office and program managers at the US-VISIT program.

On the surface, the biometric identification of the US-VISIT programs appears to be highly effective.

A NIST May 2004 report estimates that the chances that a terrorist who is on the watch list, when entering a port of entry, the chances that we catch them and have a watch-list hit is 96 percent, while maintaining a false positive rate, that is the probability that someone like you or me would nonetheless set off a watch-list hit, maintaining that probability at a mere three in 1,000.

So what's the problem? Well, the devil is in the details.

It turns out that the software systems also report and determine the quality of each image. And the software has a very difficult time in accurately matching images that have poor quality.

The premise of our study is that terrorist organizations, such as Al Qaida, will exploit this vulnerability by choosing U.S.-bound terrorists who have inherently poor image quality, such as worn out fingers, or deliberately reduced image quality.

Why is this? First, all of the information is public as found in this database; two, Al Qaida has a large pool of terrorists from which to choose from; and three, we know they're sophisticated enough.

Indeed, given the intricacies of the planning of the 9/11 attacks, I think our assumption is not only prudent but realistic.

So using publicly available information from the NIST Web site, we developed and analyzed a new mathematical model that includes red- teaming.

So first, the U.S. government chooses a biometric strategy, essentially the rules that decides how you determine if a watch-list hit happens. They choose a strategy to maximize the chances of catching a terrorist, subject to maintaining moderate congestion at the ports of entry under current staffing levels.

Then the terrorist tries to defeat this system by choosing his or her own image quality to minimize his or her chances of getting caught, and the results are sobering.

The currently implemented strategy has only a 53 percent chance of detecting a terrorist at U.S. point of entry, compared to the overall level reported in the NIST report of 96 percent.

Again, the deterioration down to a coin-flip here is due to the fact a terrorist is allowed to exploit the vulnerability in the biometric system.

So we have two main results.

The first result is that instead of using a one-size-fits-all decision rule for who gets a watch-list hit, we derived different rules for different image qualities. And by doing so, we're able to increase the detection probability from 53 percent to 73 percent -- so essentially a coin-flip up to almost three-quarters.

This is a minor software fix. Over the next few days I will give a detailed mathematical paper to people at NIST, to people at the US- VISIT office, and this should be implemented as soon as possible.

Now, even if we increased inspector-staffing levels significantly, we can't really get over the three-quarters level, over the 75 percent chance.

And here's our second result: If we take 10 fingers at visa enrollment, and then have the opportunity at point of entry to use more than two fingers for the people with the poor image quality, then we can increase our detection probably all the way up to 95 percent, without increasing the false positive rate.

Now, although switching from a two-fingerprint to a 10- fingerprint system may be costly, and certainly would be disruptive, there's simply no excuse for a $10 billion program to not achieve a 95 percent performance level, particularly given the potentially grave consequences of allowing a terrorist to cross the border.

Now, if slower two-finger matching algorithms in the immediate future cannot approach this 95 percent detection probably for poor- quality images, then the US-VISIT program should be reconfigured with 10-fingerprint scanners as soon as possible.

Thank you, and I look forward to taking your questions.

CAMP:

Thank you very much.

We just had, last week, a demonstration of some of the technology available and biometrics. They didn't have exactly the same rates. I think the way you look at your data is a little different than theirs.

But I think I understand, your concern is if people intentionally deface their fingerprints, and then on a two-finger-scan system, that's not that hard to do and they'll circumvent.

Now, if there is a bad read or an inability to read a fingerprint, there should be diversion to secondary screening at that point under the system.

But my question is more about alternative biometrics.

I've seen some demonstrations on facial scans.

I'm mean, I'm not sure that 10 fingers is really the best direction that we should go. It's almost land line versus wireless in terms of telecommunications.

But it seems to me that this facial reading has a much higher rate of accuracy, which is in sort of the development stage. As you referred to, there's other biometrics, such as eye scan.

Can you comment on those and give us some information on what you...

WEIN:

Yes. I think the operative word you bring up is "development." These are in the development phases.

I've worked on port security also with Stephen Flynn on some of these issues, and it's a hard problem, because you have all this technology that may provide a silver bullet but it may take five or six years. And the terrorists aren't going to wait five or six years to sneak a nuclear weapon in the country.

NIST has done quite a bit of analysis on face biometrics, and they claim for large-scale identification of the size we're talking about here, it simply is not a feasible option.

The iris in eyes, I've read up on all these. Some of them come promising. They may be ready in several years. They're not ready for primetime. Either they have too many false positives, people don't like to have various parts of their eyes scanned and so forth.

Whereas, it may be viewed as not wireless technology, taking 10 fingers clearly will help a lot. Indeed, my recommendations are not inconsistent with report from the NIST way back in November 2002 that two-finger methodology is simply not adequate to do large-scale identifications.

CAMP:

Well, it seems if you could deface -- yes?

(UNKNOWN)

Would you yield just for a second?

CAMP:

Yes, I will.

(UNKNOWN)

I think you were here. We had a meeting here, and they came up and told us that two fingers gave us 95 percent reliability. And you're saying that's not true because there are quality problems associated with two fingers, or any fingers, and that's why you should do 10 in order to get the higher reliability. Is that not correct?

WEIN:

The 95 percent is averaged over the entire population. The overwhelming amount of the average population, like you and me, we're not attempting to defeat the system.

Part of the reason we're putting this program in place is to stop terrorists from coming into the country. It would be naive to think that these people are not trying to defeat the system.

An insignificant fraction of people have naturally worn-out fingers, have naturally poor image quality. It's on the order of 5 to 10 percent.

CAMP:

And if I could reclaim my time, my point was, we did have a higher number. I think he's looking at a little differently. But secondly, if you can deface two fingers, you can deface 10, and that we ought to be looking at other means.

My point is that US-VISIT is just one of the items that we have to try to disrupt terrorist travel.

We also have this other biometric capability. We have the watch lists that we just had an extensive discussion on. There's inspector interviews. There's secondary screening. There's actual real intelligence that has helped disrupt.

So this is one of the many items that we're looking at in terms of how we disrupt terrorist travel.

WEIN:

I think it's important on many of these homeland security problems to move forward in two ways: One is operationally we need to get things in place that are effective and get them in there quickly, because Al Qaida and other terrorists organizations are not going to wait; and second, we need to need keep an eye

towards the future of trying to find better technologies, be they bio-sensors, be they radiation detectors, be they biometrics to help us on the five- to 10- year time line.

CAMP:

And I think the last point is that the additional fingerprints, from what we understand now, would take a great deal of additional time. And to get in this 45-second or 50-second window at the booth is very important in terms of not disrupting travel for those citizens who are not trying to do us harm.

So it is a balance there in terms of...

WEIN:

My analysis is conservative. I'm assuming each finger takes five seconds. So if you did 10 fingers, it's going to take you 50 seconds rather than 10 seconds...

(CROSSTALK)

CAMPS:

It's takes longer than 10 seconds with two fingers because of the entire process, but I understand your point. We're not there yet in terms of speeding...

WEIN:

But MITRE Tech and others at NIST and so forth have proposed the four-finger slap. And indeed, they think they can do this quite quickly, more like doing it in 10 seconds rather than in 50 seconds. And indeed, I've been told ergonomically that you actually can get better prints from the slap because your fingers are more stable.

CAMP:

Thank you. My time has expired.

I would at this time recognize the ranking member of the Border and Infrastructure Subcommittee, Ms. Sanchez, to inquire.

SANCHEZ:

Thank you, Mr. Chairman.

Thank you, Professor.

I'm trying to understand what you were telling us. Are you saying that over a large range of people -- an end (ph) sample being almost infinite or 200 million or whatever we have in the United States -- that if we look at all our fingerprints, we have a 95 percent good match. But if we're taking a look at a much smaller

of these people who we think are terrorists or would happen to be a list, that because we think that they might deform their fingers in some way or something that the percentage would therefore be lower?

I'm trying to understand how you get down to the 50 percent.

WEIN:

Right. So the 95 percent that NIST is reporting is over everyone.

SANCHEZ:

Everybody.

WEIN:

Right. So it's turn out, you know, on the order of 5 percent, let's just say, people have poor image quality. For the most part, this is naturally poor image quality, people who have worn out fingers either genetically or they scrubbed floors all their life or whatever.

Al Qaida has a large pool of terrorists to choose from to come into this country. There are pictures on the NIST Web site of what a low-image-quality finger looks like.

SANCHEZ:

So they can select those people they think are low- image people to put into the pool of people we'd be concerned about.

WEIN:

Right. So they don't even have to deliberately deface their fingers with sandpaper or chemicals or surgery or what not. They can simply choose people for their U.S.-bound missions who have poor image quality.

SANCHEZ:

And you said if we took these 10 fingers at the visa processing, when we're processing the visa, that it would take about a minute a person.

WEIN:

Well, we would take the 10 fingers at enrollment, so we would have the 10 fingers. We wouldn't need to use all 10 fingers except for the people with bad image quality. We would have that information when they show up at port of entry, "Oh, this is a person who has bad image quality. We're going to use eight or 10 fingers here at port of entry."

This can actually -- what you can do at port of entry is take 10 fingers from everyone and everything else can be blind to both the operator and to the visitor how many fingers you used to actually try to figure out if they're on the watch list.

SANCHEZ:

OK. Just wanted that cleared for my own information.

Thank you, Professor.

I'll yield back my time.

CAMP:

Thank you.

Mr. Gibbons may inquire.

GIBBONS:

Thank you, Mr. Chairman.

Mr. Wein, thank you for being here. Appreciate your testimony.

As you know, the state of Nevada, for many years, has had biometrics within their gaming industry that uses massive, large-scale recognition of large crowds, to be able to single out a selected individual based on facial recognition features.

I'm sure that their system, while not perfect, could be an ancillary or additional check for a person coming through either the screening of a port or at the same time.

But let me ask a completely different question that goes to this quality image that we talk about.

How much of the quality is outside of the control of the Department of Homeland Security? I mean, you talked about the characteristics of the fingerprint. But is there a quality issue with the machine, a quality issue with the training, a quality issue with the software?

How much of it is it outside of their control? And therefore, what portion could be corrected by going back and doing like you said, software versus the quality image of having a bad series of fingerprints?

WEIN:

Yes, that's a very good question. We asked ourselves that in the process of this research.

Unfortunately, the available data from NIST doesn't exactly answer that question, but we do have an analysis that's quite technical -- I won't go into it now -- but suggests that the great majority of this is inherent in the fingers and not as operational noise due to sweat and dirt and finger pressure and things like that.

I do think it's important to train the operators to keep the operational noise, or environmental noise, as small as possible by cleaning the fingers and cleaning the surfaces where they're putting the fingers and make sure they're holding their fingers steady and things like that.

In talking with the US-VISIT people last week, it sounds like good operations processes are in place.

So I think US-VISIT is doing all they can on the image-quality problem -- well, I mean, in getting rid of the operational noise. And most of it is simply inherent in the people, and that's why we really need to make these fixes I recommended.

GIBBONS:

Let me go back to the other biometrics, in particular facial recognition.

Is facial recognition enhanceable by increasing the number of points on a face from today's standard. What is it? Fourteen or something like that?

What if the facial recognition capability were 200 points on a given picture of a given face? Is the likelihood or accuracy of that biometric far greater?

(CROSSTALK)

WEIN:

I can just tell you that my analysis and what I will distribute in the next few days to the government sites a paper from NIST that says for large scale identification, says one to many matching for a large watch list, facial biometrics is inadequate to even help on the problem. It just isn't feasible at this point in time.

GIBBONS:

Do you know why they say that?

WEIN:

The data is there. I'd have to go back and look at the paper to give the reasons.

They mostly do a statistical analysis, look at this and conclude that the facial recognition cannot help -- it certainly is great for verification, one on one, "Are you who you say you are?" But when you're comparing to all the millions of people on a watch list, it's simply not...

GIBBONS:

Is it because of the computer technology where we have to sort through a large, massive database in order to have sufficient evidence or time or recognition features that would allow for a more accurate determination of who the individual is with something like that?

WEIN:

As I understand it from reading, there's a lot more noise involved in taking someone's picture -- the lighting, the shadows, the angle, things like that -- than there is a on a finger and why there's many more false positives.

And when you start thinking about a false positive when you're comparing against hundreds of millions of people, you're getting back to the John Doe that the assistant secretary was talking about, there's just too many John Doe's on the watch list.

GIBBONS:

It just seems to me that if we can control the quality of the fingerprint, we can control the quality of the photograph.

CAMP:

Would the gentleman yield for just a second?

GIBBONS:

Yes.

CAMP:

With the new facial recognition, the lighting is not as important as in past times. So there's some new technology there that really gets around that problem.

GIBBONS:

Mr. Chairman, my time's up.

CAMP:

If he wants to finish an answer, that's quite all right.

WEIN:

NIST has said that facial recognition has gotten much better in the last few years, but it still cannot help on the problem of large-scale identification. Maybe in five years, hopefully, but not now.

CAMP:

The gentleman from Texas, the ranking member of the full committee may inquire.

TURNER:

Thank you, Mr. Chairman.

Professor, the NIST scientists that our staff has talked to say that, if anything, your numbers are very conservative, that the quality of the fingerprint images and the terrorist watch list is even worse than what you're talking about.

So it seems to me that you're telling us something that is very, very troublesome. And I don't know how much worse -- I don't know if you've talked to them -- how much worse they think it could be than your 50 percent, or 52 percent, number.

Did they give you any indication? Have you talked to them about what they think about...

(CROSSTALK)

WEIN:

I only talked to one person from NIST was present when I briefed the program managers from US-VISIT last week.

It is true that NIST said over and over again in their papers -- that, again, are publicly available on the Web site -- that the test databases they use in some sense are much cleaner than the true operational databases that we're using to try to catch terrorists. And indeed, there's going to be lower image quality in general on the real databases than there are on these test databases.

Obviously, at this point in time they're not sharing those numbers with me, so I can't say what the magnitude of that is.

But I would agree with their assessment that my numbers are conservative and are painting, if anything, an optimistic view of the current operation.

TURNER:

I mean, this is quite disturbing. We're talking about a program that was announced in -- estimated to potentially cost the taxpayers $10 billion to put in place. And you're saying, even by your numbers, the chances of catching a determined terrorist may be only 52 percent.

WEIN:

Yes.

You know, one good thing is that a chunk of that you can get maybe from 50 to 70 or in real terms maybe 40 to 60, or whatever, by just a few lines of software code. I mean, that is part of the silver lining here.

But, yes, I do want to just iterate that a program this expensive and this important, with the implications of allowing terrorists into this country, given that there's an existing fix that we can do that doesn't involve some retrofit -- and I realize there's space constraints at the ports of entry, but this seems like a no-brainer, that we have the 10 fingers available we can get, and let's do it.

TURNER:

And so that fix, moving to 10 fingers and changing the software, would move it up to where we might have a 75 percent chance of catching a terrorist that was determined...

(CROSSTALK)

WEIN:

Yes. I think that's conservative. I would think it would be higher than that.

But, again, one would really have to almost look at the true database, and probably people with security clearance -- I don't know if NIST or people right at the US-VISIT -- would have to kind of run the final numbers.

But I think, yes, I think we would get up in the 90s.

TURNER:

We've had a large number of members of Congress raise this question about why US-VISIT is based on a two-fingerprint system rather than a 10. Some have suggested that even going to four would be a substantial improvement.

Do you understand and could you shed any light on why it is that the department chose to stay with this two-fingerprint system, which apparently is much less effective in accomplishing our objective?

WEIN:

To be honest, the last few years I've focused on other catastrophic terrorist events -- namely, small pox, anthrax, botulinum toxin and port security.

So I've only been working on this problem for the last few months. I was not engaged in this problem at the time these decisions were going on, so I would guess other people in this room are more -- would have better answer to that.

I think I'll stop there.

TURNER:

All right, my time may be up. I'm not watching -- there it is.

CAMP:

Thank you.

Mr. Dicks may inquire.

DICKS:

Well, thank you very much.

We have pointed this out to them going all the way back to the time when they were selecting contractors. And I don't know why for some reason they went for two because it was easier/faster, I think.

And I think this is something we've pointed out to them.

I think they misled the committee, Mr. Chairman. I think the witnesses that were here misled our committee by not pointing out this problem with the unrecognizable or poorly done fingerprint.

And I agree with you. I think the terrorists are going to pick that up and understand that.

I think we have to go to a 10-fingerprint system.

And I've checked with some of the best experts in the world on this, and they all agree. In fact, it was on the NIST list here (inaudible) NIST recommends a 10-slap fingerprint image stored and typed -- da, da, da.

You know, and I think Congress, I think we've put in the reports, recommending to them that they do this. Right?

(UNKNOWN)

(OFF-MIKE)

DICKS:

That they compete it and have a competitive system. They didn't do it.

And I think it's something to do with the contractor, frankly.

But having said that -- I've only got three minutes and 40 seconds -- tell us a little bit about these other issues.

We know about this one. We know this is a mistake.

You mentioned port security. Give us a couple of seconds on that.

WEIN:

I worked on the port security problem with Steve Flynn.

I think, A, that's a much more important problem in the sense it's one thing to let a terrorist in the country, it's another thing to let highly enriched uranium or a nuclear weapon into the country; B, to their credit, I think it's a lot more difficult problem, the technology isn't all there; C, I think they've been dropping the ball on this problem, that Steve Flynn and I have briefed Commissioner Bonner's entire staff. There are people there who seem to think -- they've put all their eggs into ATS basket, and we're currently testing 5 percent of the containers. The other ones can waltz through the system.

And it's just like -- I mean, it's easy for a terrorist to bypass one layer of security, particularly given the manifest rules that are in place.

We really need to do 100 percent passive radiation testing, and we need to do a fair amount of active testing in the sense of an X-ray or gamma-ray imaging to look for shielding.

And we also need to spend money now to find a way to detect highly enriched uranium, which is very difficult to catch with existing equipment.

DICKS:

You mentioned a few others, anthrax and some other ones.

WEIN:

Well, on anthrax, I have an op-ed in The Washington Post, a paper in the proceedings of National Academy of Sciences. As a result of that, your area here, Washington, D.C., if a big attack occurs, the postal workers will help distribute antibiotics throughout the area.

Hopefully, this program will go nationwide. That was a direct result of our op-ed, and it's currently funded by HHS to help them decide how, if and when to deploy the next generation anthrax testing.

My work on smallpox was instrumental in effecting the Bush administration post-attack strategy for vaccination.

DICKS:

We still don't have enough people vaccinated, though, don't we? I mean, of the caregivers, isn't that still a problem?

WEIN:

Yes. The implementation of the front-line worker vaccinating had a number of problems with it. At this point...

DICKS:

And they still haven't been corrected, have they? They still don't have enough people vaccinated, do they?

WEIN:

I think it's dead in the water at this point until we have another terrorist attack, to be honest.

DICKS:

In other words, to get more people vaccinated, the caregivers, we're going to have to have a catastrophic event in order to convince everybody do that. Is that what you're saying?

WEIN:

It may not have to be catastrophic, but I think we need another event.

DICKS:

Because nobody's paying attention? Is that what you're saying?

WEIN:

No, it's not because no one's paying attention. It's several reasons. It's the risk communication about what the risk of if I give vaccine to the front-line worker, what's the chances of them dying or having a serious incident?

It's the perception of is there really smallpox out there, the whole weapons of mass destruction in Iraq issue.

It's a complicated problem.

DICKS:

Again, I'm troubled by this, Mr. Chairman, that we've had a series of these hearings -- I commend the majority for having these hearings -- it's pointed out again and again and again the deficiencies in this homeland security program.

And I don't know how we can, and the Congress, get people's attention in the executive branch that we've got to do more on these issues, on port security, anthrax, the fingerprints for the US-VISIT program.

I mean, there are all of these problem areas that haven't been addressed. It's one of the things that's shocked me, frankly. In my service here in this Congress for 28 years, I've never seen something of this importance treated this way by the executive branch.

I commend the committee for having the hearings, because at least we have a chance to present the information to the American people, but we can't seem to get anybody to do anything about it.

I appreciate your going around and meeting with all the officials. I hope that they will respond to your very lucid presentation on this gap in the fingerprinting program. And I commend you for your good efforts. Please keep them up.

WEIN:

Thank you.

DICKS:

Thank you.

CAMP:

Thank you.

That concludes our questioning, there being no further business.

Again, I want to thank the subcommittee members and our witnesses for being here today.

The chair notes that some members may have additional questions for this panel, which they may wish to submit in writing. Without objection the hearing record will remain open for 10 days for members to submit written questions to these witnesses and to place their responses in the record.

The gentleman from Texas?

TURNER:

I just wanted to ask the chairman if he would allow me to place in the record a NIST 2002 report which concluded that the additional fingerprints, the slap system, I believe you're referring to, Professor, the time required to capture those fingerprints would be insignificant.

It goes to the heart of the issue that Mr. Dicks raised. Because I think we all have the impression that we didn't use the 10-print system because it takes too much time. And I'd like for this report to be placed as part of the record of this hearing.

CAMP:

Without objection, the NIST report may be placed in the record.

There being no further business, the hearing is now adjourned.

The FDCH Transcript Service Sept. 30, 2004

List of Speakers

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

U.S. REPRESENTATIVE DAVE CAMP (R-MI) CHAIRMAN

U.S. REPRESENTATIVE KAY GRANGER (R-TX)

U.S. REPRESENTATIVE JENNIFER DUNN (R-WA)

U.S. REPRESENTATIVE DON YOUNG (R-AK)

U.S. REPRESENTATIVE DUNCAN HUNTER (R-CA)

U.S. REPRESENTATIVE LAMAR SMITH (R-TX)

U.S. REPRESENTATIVE LINCOLN DIAZ-BALART (R-FL)

U.S. REPRESENTATIVE ROBERT W. GOODLATTE (R-VA)

U.S. REPRESENTATIVE ERNEST ISTOOK (R-OK)

U.S. REPRESENTATIVE JOHN SHADEGG (R-AZ)

U.S. REPRESENTATIVE MARK SOUDER (R-IN)

U.S. REPRESENTATIVE JOHN SWEENEY (R-NY)

U.S. REPRESENTATIVE CHRISTOPHER COX (R-CA) EX OFFICIO

U.S. REPRESENTATIVE LORETTA SANCHEZ (D-CA) RANKING MEMBER

U.S. REPRESENTATIVE EDWARD J. MARKEY (D-MA)

U.S. REPRESENTATIVE NORMAN D. DICKS (D-WA)

U.S. REPRESENTATIVE BARNEY FRANK (D-MA)

U.S. REPRESENTATIVE BENJAMIN L. CARDIN (D-MD)

U.S. REPRESENTATIVE LOUISE SLAUGHTER (D-NY)

U.S. REPRESENTATIVE PETER A. DEFAZIO (D-OR)

U.S. REPRESENTATIVE SHEILA JACKSON-LEE (D-TX)

U.S. REPRESENTATIVE BILL PASCRELL, JR. (D-NJ)

U.S. REPRESENTATIVE CHARLES GONZALEZ (D-TX)

U.S. REPRESENTATIVE JIM TURNER (D-TX) EX OFFICIO SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

U.S. REPRESENTATIVE JIM GIBBONS (R-NV) CHAIRMAN

U.S. REPRESENTATIVE JOHN SWEENEY (R-NY)

U.S. REPRESENTATIVE JENNIFER DUNN (R-WA)

U.S. REPRESENTATIVE C.W. BILL YOUNG (R-FL)

U.S. REPRESENTATIVE HAROLD ROGERS (R-KY)

U.S. REPRESENTATIVE CHRISTOPHER SHAYS (R-CT)

U.S. REPRESENTATIVE LAMAR SMITH (R-TX)

U.S. REPRESENTATIVE PORTER GOSS (R-FL)

U.S. REPRESENTATIVE PETER KING (R-NY)

U.S. REPRESENTATIVE JOHN LINDER (R-GA)

U.S. REPRESENTATIVE JOHN SHADEGG (R-AZ)

U.S. REPRESENTATIVE MAC THORNBERRY (R-TX)

U.S. REPRESENTATIVE CHRISTOPHER COX (R-CA) EX OFFICIO

U.S. REPRESENTATIVE JAMES R. LANGEVIN (D-RI) RANKING MEMBER

U.S. REPRESENTATIVE EDWARD J. MARKEY (D-MA)

U.S. REPRESENTATIVE NORMAN D. DICKS (D-WA)

U.S. REPRESENTATIVE BARNEY FRANK (D-MA)

U.S. REPRESENTATIVE JANE HARMAN (D-CA)

U.S. REPRESENTATIVE NITA M. LOWEY (D-NY)

U.S. REPRESENTATIVE ROBERT E. ANDREWS (D-NJ)

U.S. DELEGATE ELEANOR HOLMES NORTON (D-DC)

U.S. REPRESENTATIVE KAREN MCCARTHY (D-MO)

U.S. REPRESENTATIVE KENDRICK B. MEEK (D-FL)

U.S. REPRESENTATIVE JIM TURNER (D-TX) EX OFFICIO WITNESSES:

PATRICK HUGHES,

ASSISTANT SECRETARY,

INFORMATION ANALYSIS, HOMELAND SECURITY DEPARTMENT

C. STEWART VERDERY,

ASSISTANT SECRETARY,

BORDER AND TRANSPORTATION SECURITY,

FOR POLICY AND PLANNING, HOMELAND SECURITY DEPARTMENT

LAWRENCE WEIN,

PROFESSOR,

GRADUATE SCHOOL OF BUSINESS, STANFORD UNIVERSITY

Source: Federal Document Clearing House, Inc. (FDCH-eMedia, Inc.)
From **CQ Transcript Service**
No portion of this transcription may be copied, sold, or retransmitted without the express written authority of Federal Document Clearing House, Inc.
4200 Forbes Blvd., Suite 200, Lanham, MD 20706
Tel. (301) 731-1728 · Fax (301) 731-5147
©2004 Federal Document Clearing House, Inc. All Rights Reserved.