AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–760

KEEPING TERRORISTS OFF THE PLANE

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 7, 2006

Serial No. J–109–107

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

32–148 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois

MICHAEL O'NEILL, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JOHN CORNYN, Texas
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina

DIANNE FEINSTEIN, California
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
RUSSELL D. FEINGOLD, Wisconsin
RICHARD J. DURBIN, Illinois

STEPHEN HIGGINS, *Majority Chief Counsel*
STEVEN CASH, *Democratic Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	1
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	4

WITNESSES

Ford, Jess T., Director, International Affairs and Trade, Government Accountability Office, Washington, D.C.	18
Laylagian, Leon, Executive Vice President, Passenger-Cargo Security Group, Washington, D.C.	20
Rosenzweig, Paul S., Counselor to the Assistant Secretary for Policy, and Jayson P. Ahern, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security, Washington, D.C.	5

SUBMISSIONS FOR THE RECORD

Ford, Jess T., Director, International Affairs and Trade, Government Accountability Office, Washington, D.C., statement	26
Laylagian, Leon, Executive Vice President, Passenger-Cargo Security Group, Washington, D.C., statement	51
Rosenzweig, Paul S., Counselor to the Assistant Secretary for Policy, and Jayson P. Ahern, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security, Washington, D.C., statement	56

KEEPING TERRORISTS OFF THE PLANE

THURSDAY, SEPTEMBER 7, 2006

UNITED STATES SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:41 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl, Chairman of the Subcommittee, presiding.

Present: Senators Kyl and Feinstein.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Chairman KYL. This hearing of the Judiciary Committee's Subcommittee on Terrorism, Technology, and Homeland Security will come to order.

The subject of our hearing today is called "Keeping Terrorists Off the Plane," a simple title but one that is of the utmost importance, as was illustrated by events in Great Britain just about 3 weeks ago, and as we approach the fifth anniversary of September 11th next Monday.

We have a distinguished panel. Paul Rosenzweig is Counselor to the Assistant Secretary for the Policy Directorate of the Department of Homeland Security. He is also a law professor and published author with a background in litigation and public policy.

Jay Ahern is the Assistant Commissioner in the Office of Field Operations at U.S. Customs and Border Protection. He was appointed to the position in March 2003 and oversees an operations budget of $2.4 billion and over 24,000 employees. He has been in public service for over 30 years.

On the second panel, we have Jess Ford, the Director of International Affairs and Trade at the Government Accountability Office, GAO. During his over 30 years of service with GAO, he has directed the completion of numerous studies on national security and border issues for Congress, and we have one such study that we will be talking about today. And I will leave the introduction of Mr. Leon Laylagian to Senator Feinstein, but I want to thank him for traveling from New Hampshire to be with us today.

If anyone needs a reminder of what is at stake in the war against terrorists, visit the international arrival gate of any large airport in the United States. The arrivals board will show incoming flights from places like Mexico City, Tokyo, Paris, Sydney, Rio, Manila, Tel Aviv, Montreal, London. There will be a crowd of people

waiting outside the security area to pick up passengers from those flights. And the crowd will be made up of many different kinds of people, all carefully watching the stream of passengers for a familiar face, whether it is a grandparent, mother or father, child, friend, business associate. It is a place of reunions and embraces and laughter.

Of course, if the terrorists had their way, none of these people would make it to the gate alive. Given the chance, the would detonate explosive aboard an aircraft or attempt to seize control of an aircraft and drive them into targets on the ground.

We have to be clever in this war on terror—more clever than the terrorists. We have to know how to improve the security of international flights without unnecessarily disrupting travel for the many millions of people who fly into the United States each year, and without unnecessarily interfering with the work that commercial air carriers perform so well.

Obviously, one of the best places to start is by simply keeping terrorists off of airplanes. How do we do that? How well do we do it? And what do we need to do to improve?

Well, DHS has three primary tools at its disposal to screen passengers before they get on international flights. Each of these tools is in transition or experiencing problems. The first of these is the passenger name record, PNR, data. In the Aviation and Transportation Security Act of 2001, Congress mandated that air carriers share PNR data with U.S. border officials so they can get a look at the information collected when a passenger is booking a flight, run that data against terrorist and criminal watchlists, and assess risk.

Unfortunately, the European parliament has successfully challenged DHS' agreement with the European Union Commission to obtain PNR data on flights originating in Europe, and DHS and the EU are up against a September 30th deadline to attempt to reach a new agreement.

The second tool is the Advanced Passenger Information, System, or APIS. The information transmitted to the Department of Homeland Security by air carriers using APIS includes biographical data from passports presented by travelers, which CBP bounces off its terrorist and law enforcement databases. The problem is under the current regulation air carriers are permitted to transport that data up to 15 minutes after takeoff. That is 15 minutes too late if you have terrorists like those apprehended in the London bomb plot in August who want to simply blow up the aircraft in flight.

The Intelligence Reform and Terrorism Prevention Act of 2004 required DHS to issue regulations allowing for pre-departure vetting of passengers. DHS has published that regulation for comment, but it will not take effect until some time in October or later.

The third tool is DHS' Immigration Advisory Program, the IAP, which places CBP officers in foreign airports to examine the travel documents that passengers are carrying and advising airlines who is not likely to be admitted to the United States. They apparently do a very good job of weeding out travelers within invalid or expired visas and fake passports and could play an important role in deterring terrorists. However, there are presently only three IAP teams stationed abroad in London, Amsterdam, and Warsaw, with

Tokyo set to come online in October. That is too few airports, and DHS needs to aggressively expand the program.

We will also discuss today the Visa Waiver Program. The Visa Waiver Program allows approximately 16 million foreign nationals from 27 countries to enter the United States each year without first obtaining a visa. The program is extremely beneficial to the United States and our friends in the international community, but it poses a severe security vulnerability because visa waiver travelers are not interviewed and fingerprinted by consular offices before getting on planes, as those who do get a visa are.

Just this week, the Government Accountability Office issued a report raising serious issues about DHS' oversight of this program. Senator Feinstein and I just briefly talked about this on the floor a moment ago. This has been one of her chief areas of concern, and we are going to want to examine what steps DHS is taking to mitigate risks in this program. It is fortunate that countries participating in the program will be required after October 26th to issue their nationals improved e-passports, which are machine readable, tamper resistant, and carry a digital photograph and an integrated chip, but on the downside, plenty of old grandfathered passports, many of them stolen or altered, and these will continue to be accepted for international travel.

The bottom line at this point, nearly 5 years after the horrible incidents of September 2001, is that while we have taken a lot of steps to improve the security of our country, and in particular, travel from abroad on aircraft, there is obviously still a long way to go. And we know that terrorists have not been quiet during this period of time because we have too much information about plots in the works or disrupted plots that suggest that they intend to take advantage of our vulnerabilities. What this means is that everybody who is working this problem in the Government of the United States, including those of us in Congress, have got to do everything we can to identify where these creases in the system are, where the terrorists might attempt to exploit our open and wonderfully free environment for their horrible deeds and find ways to close those creases or close those loopholes. And the purpose of this hearing today is to focus on just some aspects of the problem so that as we approach this fifth anniversary, we can continue to not only engage in the oversight that this Committee has done, but also to propose any legislation or administrative fixes or anything else that we need to do to better secure our country.

Now I will turn the microphone over to Senator Feinstein. There has been nobody who has been more focused on national security, not only since September 11, 2001, but before then. I had occasion to review the list of hearings that we held before September 11th, and I do not want to say that we told you so, but Senator Feinstein and I and others had noticed a lot of things that were not right about the security and about the threats that existed to the United States. And it is no surprise, therefore, that some of the ideas that we had were very quickly passed into law after September 11th. But we did not get a whole lot of attention paid to them before.

So I could not be more privileged to have a partner in this effort more capable and more committed than Senator Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thank you very much, Mr. Chairman. I appreciate those comments, and as you know, it has been a delight for me to work with you.

I share your concerns on the Visa Waiver Program and have read the GAO report and am very concerned. You are correct, we have 27 countries, 15 million people coming in a year. The US–VISIT Program knows who comes in, but they do not know who goes out. That part of the program is not functioning. To make it worse, no one can tell us when it will be functioning. So what this leaves us with is the soft underbelly whereby people can go to a visa waiver country, which there are 27 of now, and come in just with a passport.

What complicates this is there is so much fraudulent passport use, and I want to read one sentence from the GAO report right at the beginning: "Stolen passports from visa waiver countries are prized travel documents among terrorists, criminals, and immigration law violators, creating an additional risk. While the DHS has intercepted many fraudulent documents at U.S. ports of entry, DHS officials acknowledge that an undetermined number of inadmissible aliens may have entered the United States using a stolen or lost passport from a visa waiver country."

Now, I am privy to intelligence data. I cannot give you the numbers, but I can tell you there are tens of thousands of these documents stolen—passports, Geneva Convention travel documents, and international driver's licenses. These become prime acquisitions for terrorists because they can simply come in from a visa waiver country with these documents.

The report goes on: "DHS has sought to require the reporting of lost and stolen passport data to the United States and the International Criminal Police Organization (Interpol), but it has not issued clear reporting guidelines to participating countries." My question of DHS is: Why not?

Secondly, while most visa waiver countries participate with Interpol's databases, four do not. DHS is not using Interpol's data to its full potential as a border screening tool because DHS does not automatically access the data at primary locations. Again, why not?

Senator Sessions and I got into the immigration bill a passport fraud bill, Senator Kyl, which toughened the penalties for passport fraud. When we began to look into it, somebody that had a fraudulent passport was simply given the passport back and let go. My view is there has to be a price for the use of a fraudulent passport, and it ought to be a "go to jail free" ticket. We toughened the penalties. That is part of the immigration bill that apparently isn't going anywhere right now. My thought was that you and I and the Committee might put this part out as a stand-alone, as we did our border tunnel bill, and just get it passed before we go out in October. So that is one thought that just germinated through my head.

But in the 14 years I have been on this Committee and on the Immigration Subcommittee, we have had testimony about the Visa Waiver Program, and it has been one delay after the other in terms of setting up and getting effective the US–VISIT Program. I am

very worried about it. We now have people who think, well, you will introduce a bill and let this country or that country come into the Visa Waiver Program. And I feel very strongly that if a country does not meet the statutory requirements for visa waiver, they should not be allowed to come into the program. This again, I repeat, is the soft underbelly.

Now, let me comment on one other point that is coming to my attention, and that is the issue of cargo security aboard passenger planes coming into the United States. Every day passengers remove their shoes, take out their laptops, leave liquids behind, bags pass through electronic screeners, and everybody accepts this as a necessary inconvenience. And we have all stood in the lines and watched this happening, and I think it is one of the great things about America, that people just heave to and say, look, if it helps make things secure, I am prepared to stand there for an hour, an hour and a half. And so all the passengers really get my very serious commendation.

But on some level, this provides a false sense of security. Recent news suggests that only 10 to 15 percent of air cargo is screened for explosive, even though this commercial air cargo gets stowed in the same compartments of passenger airplanes as checked luggage. This, in my view, is unacceptable and also unnecessary, especially given the other means of transportation often available for cargo transportation, including all cargo airplanes.

My view is very firm. If we cannot get more cargo screened, we ought to prohibit it on passenger airliners and let it go somewhere else. But we have got to screen cargo because this, again, is another part of the soft underbelly of the Nation. And so I hope to ask some of these questions of our witnesses. I want to welcome them here and not prolong them any longer.

Chairman KYL. Thank you very much, Senator Feinstein.

We will start with our two witnesses. We will start, Mr. Rosenzweig, with you and then Mr. Ahern. The clock says 5 minutes. If you can keep it roughly to that, that would be great. Of course, your written statements will be included in the record.

STATEMENT OF PAUL S. ROSENZWEIG, COUNSELOR TO THE ASSISTANT SECRETARY FOR POLICY, AND JAYSON P. AHERN, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. ROSENZWEIG. Thank you very much, Chairman Kyl, Senator Feinstein. I will keep to 5 minutes, though I will look forward to the questions and answers, since some of the answers to many of the questions you and Senator Feinstein have posed in your opening will take somewhat longer than 5 minutes for me to address.

I am very pleased to be here today to discuss the ongoing efforts of the Department to prevent terrorists from entering the United States and posing a threat to international air travel. As you noted, the recently dismantled plot to blow up aircraft en route to the United States from Britain reinforces the importance of the homeland security mission. It reminds us not only that terrorists remain intent upon targeting air travel, but also of the importance of a layered approach to security. I will be happy to address all of the pro-

grams that we have spoken of in the questions and answers. In my brief remarks now, I would like just address the Visa Waiver and the PNR—Passenger Name Record—program.

As you know, the Visa Waiver Program allows citizens from 27 designated countries to come to this country for up to 90 days without a visa. VWP is at the forefront of our efforts to facilitate international travel. Millions of people use it every year. It is also at the forefront of our effort to defend against those who would abuse America's welcoming nature.

The program sets strict security standards for member countries. For instance, visa waiver country passports have to contain a chip with the user's biometric and biographic data, a requirement that has been propagated over the past several years. Also, VWP travelers are required to enroll in the US–VISIT Program upon arrival, which collects their fingerprints and photographs and stores them. We have been moving forward on developing protocols for the reporting of lost and stolen passports, and to maybe make a bit of news, I can say that they have been cleared through the Government, and we anticipate rolling them out with an expectation of asking our EU colleagues to meet the new standards by April of next year. We have been coordinating with the Department of State on a series of bilateral approaches to the various countries to inform them of the new standards, and I will be happy to elaborate on what they are likely to be during our discussions.

Just this week, as you alluded to, GAO did issue several reports on the Visa Waiver Program. We appreciate the GAO reports and their recommendations for improvement. In fact, we have already addressed many of the issues GAO has identified. We have made good progress. There is, however, still room for improvement, and most saliently, the current VWP program identifies security threats exclusively on a country-by-country basis. We think that, as we go forward, the program needs to look for security threats on a passenger-by-passenger basis. We look forward to working with the Senate and with our international partners to strengthen VWP's security features.

The second issue I would like to mention is Passenger Name Records. That is airline information that tells us about a passenger's identity and travel plans, for example, information about itinerary or contact phone numbers. Federal law requires that airlines turn over PNR to the Department, and we currently collect it from 127 airlines. that number represents essentially every major carrier that flies to the United States. The depth and breadth of PNR makes it a vital tool for the thorough vetting of all passengers.

As you also know, however, European officials have expressed misgivings about the status of the program under European private laws. The U.S.-EU arrangement on PNR data sets strict limits on our ability to share PNR information, both within the Department of Homeland Security and with other counterterrorism and law enforcement agencies. And in May of this year, the European Court of Justice annulled the agreement based upon its reading of European law. DHS is strongly of the belief that continued sharing of PNR data is essential for safe and secure international travel. At

the same time, we are committed to making sure that air travel is not disrupted by these events.

As we negotiate with our European allies for a replacement agreement, we will not forget the key lessons of 9/11: the necessity of sharing information so dots can be connected before attacks materialize. The two programs I have highlighted stand at the front and center of DHS' effort to prevent terrorists from entering the United States and posing a threat to international air travel. The information provided through the VWP and PNR, as well as through API and the IAP program you have mentioned, are essential to our homeland security efforts.

Mr. Chairman, Senator Feinstein, I want to thank you for the opportunity to present this them, and I look forward to responding to your questions.

Chairman KYL. I appreciate it. You have a lot to cover, and 5 minutes does not do it justice. We will get back to you. Thank you.

Mr. Ahern?

Mr. AHERN. Thank you very much, Chairman Kyl and Ranking Member Feinstein. It is my pleasure to appear before you today and discuss the efforts of U.S. Customs and Border Protection and what measures we have taken to increase the security and to protect the country against the threat of terrorism.

First I would like to speak about our progress that we have made in enhancing security at our ports of entry, with a particular focus on aviation security. And, secondly, I would like to explain CBP's critical role in response to the recent threat to aviation for flights departing the United Kingdom destined for the United States where this plot to blow up commercial aircraft reinforced the threat that this country continues to face today.

To put our mission in perspective, and certainly both Senators being from Arizona and California, you realize that the Border Patrol, another operating component within CBP, annually apprehends over 1 million illegal aliens attempting to enter the country illegally between our ports of entry. And certainly that is a considerable challenge. But I would submit that the activity in our Nation's ports of entry is just as daunting and poses other challenges. In this environment, we have to use risk management in order to determine which travelers are legitimate and law-abiding versus those that are attempting to circumvent laws.

The universe is, for example, in 2005, fiscal year 2005, we had 431 million people, travelers applying for admission coming into this country at our ports of entry. And although this is a largely compliant population of travelers, we actually had 565,417 people, individuals who were found to be inadmissible to the United States for a variety of adverse reasons. But most alarming is the fact that CBP detected 493 of these individuals to be inadmissible under suspicion of terrorist or security grounds. These include, in addition to the thousands of other arrests that we make at our ports of entry for narcotics and other violations of law, 7,662 criminals that were queried through the National Crime Information Database. And the number is significant as it continues to go up, but it points to one of the other enhancements that have been made since 9/11, and that is just not querying people solely on the biographic information but also using the biometric capabilities we now have at

our ports of entry to identify individuals who may be traveling across our borders with aliases so we can actually do the biometric confirmation of who they are and confirm the warrant at that point in time.

But speaking of the specific U.K.–U.S. threat, on August 9, 2006, this year, we were faced with a very serious threat to the security of our country and its citizens, and the thwarted London-based attacks certainly reminded us all that we must remain vigilant and continue our efforts in the detection and apprehension of potential terrorists before they step foot on a plane, in advance of their departure, and in advance of their arrival into the United States. And as our front-line border agency, CBP was rapidly responding to these threats by immediately implementing a pre-departure vetting process on all flights—that is approximately 130 flights a day—from all airports in the U.K. that are destined to the United States.

In order to accomplish this critical homeland security measure, CBP has been successful in large part due to the outstanding cooperation we have with our partners in the airline industry. In responding to these threats, we required the commercial carriers to provide Advance Passenger Information system, that data, in advance of departure, and CBP at our National Targeting Center then completed a thorough vetting of each individual against a multiplicity of systems, including terrorist watchlists and our Treasury Enforcement Communications System. This individual vetting required biographic information that was cued through an electronic swipe of the passport by the airlines overseas—again, pre-departure. Once the vetting was complete, we then would provide the information back to the airlines to be able to give an all-clear, or if those individuals were not allowed to board, that was then coordinated appropriately with the U.K. government authorities. In a recent example, 3 days ago, on September 4th, through this process we actually identified an individual who was on the no-fly list prior to departure. He was given a no-fly and actually was turned over to the authorities in London before boarding for the United States.

Just to summarize the amount of flights that have been vetted since the August 9th threat stream, 3,597 flights have been vetted coming into this country, and they were carrying 769,000 passengers destined to the United States. Of that population, 20 individuals were denied boarding for terrorist or security grounds pre-departure. That shows how critical it is to get the information prior to boarding on aircrafts bound for the United States.

Given this process overseas, this is why DHS and CBP provided the Notice of Proposed Rulemaking—and it is currently posted in the Federal Register—that proposed to seek the Advance Passenger Information 60 minutes prior to departure or through an Advance Quick Query process real time up to 15 minutes prior to departure if the 60-minute requirement cannot be met because of transiting passengers at major international gateways. And this certainly is essential, as demonstrated by the U.K. plot, to make sure that we have this information in advance of departure so we can do a thorough vetting.

I will certainly begin to summarize at this point because I do not want to go beyond my time, but I will be happy to talk about the

Immigration Advisory Program that you spoke of that we have in three locations. We will have a fourth location up within a very short period of time, and we have an additional expansion plan for fiscal year 2007. And at this point in time, I will conclude and look forward to any questions you might have.

[The prepared statement of Mr. Rosenzweig and Mr. Ahern appears as a submission for the record.]

Chairman KYL. Well, thank you again. There is far too much for you to cover everything.

Let me begin by just focusing, Mr. Ahern, on the last thing you talked about. There has been some publicity about the problems associated with aircraft that take off where there has not been an adequate opportunity to vet all of the people on the manifest prior—or on the passenger list prior to takeoff. You described a rulemaking or mentioned a rulemaking that would expand this. Would you tell us what the status of that is, what you expect to come from it, and what will occur as a result?

Mr. AHERN. Yes, sir. I would be happy to, Senator. Currently, the requirement that is provided to the carriers is to give the information, the Advance Passenger Information, which is all the information basically contained in a passport, electronically transmitted, the passenger manifest, if you will, so we can then run it against all our watchlisting systems. But, currently, that is mandatorily required 15 minutes after—upon wheels up, 15 minutes after wheels up. That we have seen through many of the flight diversions that have occurred on aircraft bound for the United States, that is too late in the process. And given the current threat stream that we are still working right now, that clearly would have been too late.

So the Notice of Proposed Rulemaking went in about 2 weeks before the August 9th threat, and we actually have it proposed for getting the information 60 minutes prior to departure, but also through deliberations and very exhaustive discussions with the airline industry, who have been very supportive of this, we have learned also a lot of transiting passengers in major international gateways, we had to take a look at how could we make sure we do not negatively impact the airline industry as we impose this new rule.

So we were able to come up with something that still provided a level of security pre-departure, which is called the Advance Quick Query, so that we can actually get real-time submission and provide real-time response, but closing it out 15 minutes pre-departure so that we still can make security vetting determinations prior to the aircraft pushing back.

The public comment period closes on October the 12th. We will analyze those comments, and then we will move forward with the final implementation of the rule.

Chairman KYL. And that seems logical that for 95 percent of the passengers, there is plenty of time to get the pre-screening done, and for the few that come in at the very last minute, you could do some real-time checking, and it wouldn't be too burdensome. I mean, that is at least the way I look at it. Is that the pitch you are making on the rulemaking?

Mr. AHERN. That is exactly what we are stating at this point, and that again is something we have learned through a very delib-

erative process with the airlines. We do not want to have a negative impact on the airline industry and have the economic harm be created through this rulemaking process.

Chairman KYL. Just one more question of you. You mentioned the fact that there had been 20 people detained as a result of the interlocking checks that you described, and I will get to that later. But what can you say about these 20 people?

Mr. AHERN. A lot of these individuals were people that were on either no-fly or watchlisted individuals. Whether they actually posed a threat to civil aviation security, I would not go into detail in this particular hearing. I could say they were not part of the U.K. plot. Those individuals had previously been disrupted by the U.K. authorities. But these were individuals that presented security concerns, and we thought it was prudent to give a denied boarding and have them offloaded and turned over to the U.K. authorities.

Chairman KYL. Okay. I did not think you could tell us much about them, but at least it illustrates the fact that something has to happen, and for the general public, who knows what might—some may be fine, others may not.

Mr. Rosenzweig, you talked about the Visa Waiver Program, and I am going to, since that has been such an interest of Senator Feinstein's, leave most of that for her to get into, if she would like. But you talked about some new standards in April. Those I gather will make the passports themselves more secure, but would not do anything to solve the problem of, number one, the passports that have been stolen already, or manufactured; and, two, the lack of an oral interview, which is at least supposed to occur with the issuance of a visa and which sometimes can reveal information that is important for screening purposes. Is that correct?

Mr. ROSENZWEIG. That is, I guess, one of the problems with speaking too quickly. I must misstated it slightly. The standards that DHS will be pushing out to our friends and colleagues in the European Union for which we will seek action by next April will be standards by which we ask them to do direct reporting of lost and stolen passports, both blanks and stolen issued travel documents, in a direct report to the United States. It will encompass both a time requirement and a request that they provide a 24/7 point of contact within their government since we need somebody that we can reach on a real-time basis to resolve ambiguities when a document that we think meets—is lost or stolen is encountered by one of our CBP agents at the port of entry.

So that is the standard that I was speaking about. It is the one that is directly responsive to the Enhanced Border Security Act.

Chairman KYL. I think you described it correctly. I mis-described it a moment ago. And this is a problem because in the past we had not gotten notice from many countries of stolen passports. Is that correct?

Mr. ROSENZWEIG. That is correct. We have been working with them to develop means for direct reporting, and then the secondary goal is the one alluded to by Senator Feinstein, which is to make it available at ports of entry to the CBP officer on the ground so that he can detail and use that on a minute-by-minute basis.

Chairman KYL. But it is still a fact that many passports are stolen. That is still remains a problem. And, secondly—and I am going to get into the interlocking other mechanisms here in a minute, but there is no independent interview of the person coming here.

Mr. ROSENZWEIG. That is correct.

Chairman KYL. And just to illustrate the nature of this problem, Zacarias Moussaoui, who was the suspected 20th hijacker, was a French citizens, as I believe. Is that correct?

Mr. ROSENZWEIG. Yes.

Chairman KYL. And I don't recall whether he came here under the Visa Waiver Program, but he could have if he did not. And I am getting nods of heads that yes, he did.

There is something about this clock that is giving me far more time than I deserve, and I do not know quite what it is. So what I will do, Senator Feinstein, is turn to you if you are ready, and then we will come back for another round.

Senator FEINSTEIN. Okay. Thank you very much, Mr. Chairman.

I think to Mr. Rosenzweig, let me ask this question: The GAO report concludes that the Visa Waiver Program would be strengthened if DHS takes certain steps, including requiring that all visa waiver countries provide the United States and Interpol with nonbiographical data from lost or stolen issued passports as well as blank passports, and also development of clear standard operating procedures for the reporting of stolen and lost blank and issued passports. It also recommend that DHS develop and implement a plan to make Interpol's stolen travel document database automatically available to immigration officers at primary inspection.

What steps is DHS taking to implement that recommendation?

Mr. ROSENZWEIG. Thank you very much for the question. The news is good, albeit perhaps a little delayed. On the first of those, the development of uniform standards for reporting, that is precisely the set of standards that I was speaking about with Senator Kyl. We expect to have those cleared out of the executive branch within a matter of weeks.

Senator FEINSTEIN. Is this the April release that you were talking about?

Mr. ROSENZWEIG. April will be the deadline that we would be asking our European colleagues to meet. I expect for them to have these standards in hand and to be sharing them with them as we go through the fall, recognizing that it is not an instantaneous process that they can turn on on a dime. We are going to ask them to—

Senator FEINSTEIN. Why don't you give us—it might be useful—the operational date. When will this be operational?

Mr. ROSENZWEIG. We are going to ask our European colleagues who are members of the Visa Waiver Program to have this done by April 30, 2007.

Senator FEINSTEIN. So it will be operational May 1?

Mr. ROSENZWEIG. That is our request. Whether or not all of the visa waiver countries meet that deadline and how we will deal with—

Senator FEINSTEIN. I guess this is the problem. No deadline is ever kept, and I cannot think of one that has been kept with this program. So, I mean, I really think this is important, and I think

if a visa waiver country does not want to cooperate, they should drop out of the system.

I think we are in an era now where I understand airlines want passengers. I understand the chamber wants business, but American citizens do not want terrorists. And, therefore, this becomes much more important than anything else.

Mr. ROSENZWEIG. I agree with your sentiments. We are not in a position to make a unilateral demand, and the only hammer we have is the rather stringent one of compelling a country to drop out, which has very significant foreign policy and—I am not apologist for the visa waiver countries. I think that they need to get with the program. But I cannot make them—

Senator FEINSTEIN. There ought to be statutory regulations, and if somebody does not want to follow them, then they drop out of the program. Nobody forces a country to be in the Visa Waiver Program.

So, I mean, I guess people can sort of develop a great affront and say, "Oh, I am appalled by this." But, look, this country has been attacked in a major way, and we care about it. I guess it is the largest—it is a larger loss of life than Pearl Harbor. So, you know, people are concerned. They do not want it to happen again.

So the stolen passport becomes a very interesting terrorist expediter, and we have got to control it. So, I mean, my view is that if you run into recalcitrant countries, please—I do not know how Senator Kyl feels about it, but I sure feel strongly. I would be willing to introduce the legislation. Whether it would go anywhere I cannot tell you, but—

Mr. ROSENZWEIG. Well, I am quite certain that this colloquy will find its way into the capitals of the visa waiver countries, and I will certainly make sure that they are aware that I share your concerns.

Chairman KYL. Senator Feinstein, would you just yield for a second, and then I will give you more time.

Senator FEINSTEIN. Yes, of course.

Chairman KYL. Mr. Rosenzweig, what four countries do not share lost or stolen passport information with Interpol?

Mr. ROSENZWEIG. I have that in my briefing book, but I am just going to—

Chairman KYL. Okay. We might as well just get their names out right here.

Mr. ROSENZWEIG. Holland, Japan, Norway, and Sweden.

Chairman KYL. All right. Holland, Japan, Norway, and Sweden.

Mr. ROSENZWEIG. Yes.

Chairman KYL. And regarding your request in 2005 to certify their intention to report lost or stolen passport data to DHS, what countries failed to certify their intent to share that data?

Mr. ROSENZWEIG. I do not believe any country failed to certify their intent to share that data.

Chairman KYL. All right. Double-check that for us.

Mr. ROSENZWEIG. Yes, we would be happy to get back to you.

Chairman KYL. Okay. Thank you.

Go ahead, Senator Feinstein.

Senator FEINSTEIN. Those are very good questions. Let me follow up. When will American inspectors at airports have full access to Interpol data on passports?

Mr. ROSENZWEIG. That is the second part of your earlier question. We completed a pilot test on historical data with the Interpol database through something known as the Mind Mobile Interpol—

Mr. AHERN. Network Database.

Mr. ROSENZWEIG. Network Database. Thank you, Jay— just this past July, and we are analyzing the results. That test actually demonstrated some operational difficulties in making a live connection to Interpol that need to be resolved. My goal would be to have those resolved, at least in theory, by the end of this year and then operational in the second or third quarter of next year. That is an aspirational goal. I should add—

Senator FEINSTEIN. Of 2006? I am writing it down, and I am going to get you to sign it afterwards.

Mr. ROSENZWEIG. Absolutely.

Senator FEINSTEIN. Operational when?

Mr. ROSENZWEIG. My goal is second or third quarter of next year, 2007.

Mr. AHERN. Senator, if I might add a little more, give my colleague here a break for a second, if I might, some of the things that are happening I think that are important to make sure for the record it is reflected that we get a considerable amount of lost and stolen passport information directly into our systems today through the State Department. We also get a direct feed from the U.K. Government to the State Department on lost and stolen passports. So we have a considerable amount of lost and stolen passports in our system today, so that is fed in through the Department of State's class system into our integrated border inspection system. So we do have access to a considerable amount.

Certainly, we look forward to getting the full link with Interpol, but even with Interpol, I think there is an important thing that we need to make sure as we go forward, and certainly, we realize, as does the head of Interpol, that we need to make sure there is a good quality data in that system, to make sure that it is updated and current, because a lot of reported lost passports get retrieved. And even in the U.K. flight vetting, as we were looking against some of the lost and stolen passport database access we do have, we found a lot of individuals who had reported a passport as being stolen that had later been retrieved, and we were then doing an interview with these individuals on the basis that it was a lost document, and they just had not reported its retrieval.

So we need to make sure that the quality of the data that is put into the Interpol database and we then have access to is well defined and accurate and current.

Senator FEINSTEIN. I would be willing to make a bet that your numbers will not come anywhere close to the number stolen in a given year from EU countries that are members of the Visa Waiver Program.

Mr. AHERN. I do not want to debate that fact with you. I just wanted to talk about where it is—

Senator FEINSTEIN. You do not want to do that, because it is a huge number. And that is really the concern because—why would

somebody steal these passports? Only one reason: to sell them on the black market to somebody who could not get a passport legitimately.

Mr. AHERN. That is clearly the purpose, to gain illegal access into some country.

Senator FEINSTEIN. Now, I asked the question about American inspectors at airports, but let me put it another way. Would this include all primary immigration inspectors, Mr. Rosenzweig? The earlier question I asked about having that available.

Mr. ROSENZWEIG. You mean the access to the Interpol lost and stolen database?

Senator FEINSTEIN. Yes.

Mr. ROSENZWEIG. In the long run, yes, as with—

Senator FEINSTEIN. But that is not in your date of the second or third quarter of next year. That is just airports.

Mr. ROSENZWEIG. That would be for airports, yes.

Senator FEINSTEIN. Okay. Then we have ports of entry, shipping ports of entry.

Mr. ROSENZWEIG. Yes. The plan, of course, would be to propagate it from air ports of entry and sea ports of entry, which are relatively minor and modest. But land ports of entry are an amazingly numerous and difficult task, and, of course, it requires technology, it requires an investment of a substantial amount of money, and it will require deployment and training. It will not be instantaneous.

Senator FEINSTEIN. Let me just conclude by thanking you for your work. I know it is hard because I know there are cross-conflicts, and you are caught right in the middle of them. But it is just so important—this country has been such a sieve—that we close some of those doors.

I was telling the Senator, the Chairman, I should say, that even before 9/11, I had been very concerned about the misuse of the student visa program, and I could not get anybody's attention. We had some evidence that there was a lot of fraud going on, even a bogus school set up next door to one of our offices in California. You had California officials at schools convicted of falsifying information about foreign students present that were not present. And then just recently, I saw where 11 students from Israel did not show up at the university, the University of Montana, I believe it was.

Chairman KYL. Egypt.

Senator FEINSTEIN. Excuse me, Egyptian students did not show up at the University of Montana, which raises a whole question about how this program is being monitored, if, in fact, it is. Do you have any information on that?

Mr. ROSENZWEIG. We track students through our SEVIS program, the Student Entry Visa Issuance System. My familiarity with the 11 Egyptians that you were talking about comes only from the same place it does with you, which is the newspaper—or perhaps you have better information than I. I do know that we track them down.

We continue through Immigration and Customs Enforcement to register schools within the SEVIS program as recipients of students. The issuance of visas to students, though, is a responsibility of the Department of State out in the various posts, and so I would

probably have to defer on who is getting issued and what the standards are to somebody from that Department.

Senator FEINSTEIN. Would you be willing to take a look at it and give us a report in writing as to how it is now being monitored and whether, in fact, it is?

Mr. ROSENZWEIG. Absolutely.

Senator FEINSTEIN. I think the universities finally came to the table and agreed to monitor students to see first, if they were accepted, if they came, and then to send that information to INS; secondly, that they remained in school and actually took the courses, and check—I do not know whether it was by quarter or by year, but it was one of the two. And I think that is very useful.

We know that the student visa programs were used by terrorists who actually committed attacks on this country, so I think it is something that is well ordered.

Mr. ROSENZWEIG. I would be happy to get back to you.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman KYL. Thank you, Senator Feinstein.

For either one of you, why can't DHS do more to get Passenger Name Record data on transatlantic flights? Going back to something I talked about in my opening statement.

Mr. ROSENZWEIG. I think that one is in my square. We do get Passenger Name Record information on transatlantic flights. However, because of European concerns about privacy issues, the Department is prohibited, except on particularized case-by-case bases, from sharing that information with anybody outside of the Customs and Border Protection. So, for example, CBP cannot share that information with Immigration and Customs Enforcement, much less the FBI or other counterterrorism or counterintelligence agencies. That has, as Secretary Chertoff has said, placed some very significant limits on our ability to use that data to assess terrorist threats from unknown terrorists—cleanskins. Where we use API, Advance Passenger Information, for known terrorists, watchlist matching, the Passenger Name Record is principally of use for us in identifying the unknown terrorists.

The European Court of Justice has just struck down the agreement that limited our ability to use Passenger Name Record data, and, indeed, my boss is in Europe today trying to negotiate a replacement.

I have to say that European privacy concerns are tending to pull us to use even less of the data, if I read the members of their parliament correctly. That I think would be inconsistent with American interests in making better use of that data as a vital means of identifying who is coming.

Chairman KYL. Isn't the problem here that not everybody is known to be a terrorist who is a terrorist? Sometimes you have to put a few things together to connect the dots, as the saying goes, to figure out that this person is probably not somebody you want to allow to get on the airplane and come to the U.S., or at least you want to check some additional things before you do that. So given the fact that there is an awful lot of gray in here, you do need to share that data, say, with the FBI or someone else to say, "Do you know anything about this person? Is there a problem

here?" Is that the problem? And if so, what can the United States do, what could the Congress do to persuade our European friends who are, for the most part, on the Visa Waiver Program that this is something they need to help with?

Mr. ROSENZWEIG. Well, I am going to let Mr. Ahern tell you a little bit about the actual uses because I think that is an important point.

On the second of those, that is the argument that I made as recently as this morning to members of the EU, that enhanced data sharing is the foundation of the Visa Waiver Program, and that our ability to get information about individuals so that we can target our resources better allows us to be more forthcoming and facilitative in the travel sphere, and that the converse of that is equally true.

Jay?

Mr. AHERN. Senator, certainly you have hit on a real critical issue, and that is the ability to identify individuals who are not watchlisted and who could be associated with individuals who may be. And one of the things that the Passenger Name Record system provides us is a research capability. Currently, 127 airlines that fly to the United States provide that information to us. That actually accounts for 95 percent of the air travel. Before there is any alarm over the 5 percent that remains, that is very small or charter airlines that do not have a reservation system, and so they are not able to comply with the existing law. But the ability to take it and put links and have our tactical targeters at the National Targeting Center or through the local targeting units we have throughout the country, to be able to do linking of individuals on reservations is critical for us for national security because, as we find more people look for individuals that are not watchlisted to try to introduce them into the country, it is a critical national security tool that we have to have.

Chairman KYL. Let me just ask one final question here relating to the additional resources that might be provided to the Visa Waiver Program Oversight Unit. There has been publicity about the small number of people at headquarters who are available to provide oversight, and I would be anxious to get your ideas about what we can do. Is it necessary for us to authorize something here or to appropriate more money or to direct that more people be put into the oversight position? Because, again, this is a program which is designed to operate to make it easy for people when you do not have the usual checks of, for example, the oral interview that is required for the visa issuance.

Mr. ROSENZWEIG. I believe that at this point I am supposed to say the President's request for funding for fiscal year 2007, which I believe the current appropriations bill meets, will, we think, cover our resource needs. We operate with full-time staff in my office as well as several contractors who provide assistance. We also call upon the resources of ICE and CBP agents overseas to participate in the country reviews. So at this juncture, we are confident that the President's request, if fully funded, would meet our needs for the—

Chairman KYL. Well, how many people are in the headquarters right now to oversee this program?

Mr. ROSENZWEIG. The Visa Oversight Unit has two full-time staff and—three contractors?

Mr. AHERN. Three contractors.

Chairman KYL. See, that is the problem. That is the question I got this morning on an interview. How can they possibly do this with two? I said, "Gee, I do not know. I will ask this afternoon." I mean, it seems implausible that with the number of millions of passengers and the difficulties—and we have only scratched the surface here in the brief time we have today discussing that—that that is an adequate number. And so I guess I would be curious when you say that the new budget submission will provide adequate resources, how many people will that provide? And I realize people are not everything. A lot of it is the technology as well. But how many would you have overseeing it?

Mr. ROSENZWEIG. Perhaps I should clarify that the five people here in Washington are not the ones responsible for each country review. Before we review Norway's compliance or Brunei's compliance, we assemble a team comprised of other DHS employees and also contractors, give them training on the country conditions, and then send them out for an intensive 2-week study of a particular country's security arrangements, passport issuance processes, et cetera. So the five people that you and I are discussing are essentially the administrative, bureaucratic head back here in Washington. They are not the arms and the legs who are responsible for all the millions of people. In addition, we call upon many other resources at CBP and in the Policy Directorate to do things like meet with Interpol to discuss the integration of lost or stolen—of their stolen travel documents database into Customs and Border Protection.

Chairman KYL. Why don't you simply, if you would, submit for the record a little statement that provides the justification or the rationale for the number of positions sought in the new budget submission.

Mr. ROSENZWEIG. I would be happy to.

Chairman KYL. And any other information that you think would be useful to us.

I have some additional questions I will ask you, if I could, for the record, and we will leave the record open for you to not only answer those questions, but if other members of the Committee have questions they might want to submit, you will receive those as well.

Senator Feinstein, anything else of these witnesses?

Senator FEINSTEIN. No, I have nothing else. Thank you.

Chairman KYL. There is so much more we could go into, and I am sure there is a lot more you would like to tell us. We have another panel, and we are constrained by time. But please, if there are other things that you think you need to bring to our attention to provide a complete picture, do that as part of your submission in the questions that we will get to you. And I want to thank you both, as Senator Feinstein did, for your service. Please pass that on to the folks that you work with as well.

Mr. ROSENZWEIG. Thank you.

Mr. AHERN. Thank you.

Chairman KYL. Thank you very much.

Chairman KYL. While this panel is retiring, I will again mention that Jess Ford is the Director of International Affairs and Trade at the GAO, and we have reports and some questions of him, and I will allow Senator Feinstein to introduce for the record our other witness.

Senator FEINSTEIN. The Chairman has graciously asked if I would introduce Leon Laylagian, and I am very pleased to do so. He is the Executive Vice President of the Passenger-Cargo Security Group, which is a nonprofit trade association. He is a pilot of 757s and 767s, as I understand it; first officer; a graduate of Embry-Riddle Aeronautical University; he previously served the Air Line Pilots Association as a security liaison; and a former representative of the Coalition of Airline Pilots Associations and the Independent Pilot Pilots Association. He has also served as a member of TSA's Aviation Safety Advisory Committee for cargo security in 2003.

Chairman KYL. Thank you.

Mr. Ford, would you like to begin? And then we will just turn directly to Mr. Laylagian, and then have our questions.

STATEMENT OF JESS T. FORD, DIRECTOR, INTERNATIONAL AFFAIRS AND TRADE, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, D.C.

Mr. FORD. Thank you, Mr. Chairman and Senator Feinstein. I will try to be brief. You have already covered some of the main points in our reports, which were issued on Tuesday. I am pleased to discuss these reports.

In fiscal year 2005, nearly 16 million travelers entered the United States under the Visa Waiver Program, covering 27 participating countries who are allowed to come here for 90 days or less without obtaining a visa. Participating countries were selected because their citizens had demonstrated a pattern of compliance with U.S. immigration laws and the governments of these countries granted reciprocal visa-free travel to U.S. citizens. The Visa Waiver Program was created in 1986 as a pilot program and was made permanent by law in 2000.

The Visa Waiver Program facilitates international travel for millions of foreign citizens seeking to visit the United States each year, creating substantial economic benefits to our country. However, travelers visiting the United States under the Visa Waiver Program can pose significant security risks, for example, because they are not interviewed by a consular officer prior to their travel. In addition, border inspectors at U.S. ports of entry may not know the visa waiver traveler's language or their local fraudulent document trends in the traveler's home country, nor have the time to conduct an extensive interview.

Lost and stolen passports from visa waiver countries are highly prized among travelers seeking to conceal their true intent and identities and nationalities. DHS officials have acknowledged that an undetermined number of inadmissible aliens may have entered the United States using stolen or lost passports from a visa waiver country. In fact, passports from the Visa Waiver Program countries have been used illegally by hundreds of travelers attempting to enter the United States.

For example, we reported that from January to June of 2005, approximately 300 individuals had their passports confiscated at the border because they were considered to be fraudulent. In 2002, Congress mandated that the DHS review the security risks poses by each of the visa waiver countries' participation in the program at least every 2 years. In 2004, DHS conducted its first mandated biennial reviews of 25 of the 27 member countries and subsequently determined that all of them should remain in the program.

However, we have identified several problems with the country review process. Specifically, key interagency stakeholders, such as the embassies overseas and DHS forensic document analysts, were left out of portions of the review process. Also, the country assessments prepared by DHS were not completed in a timely fashion and contained some dated information that did not necessarily reflect current risks. For example, they conducted the review from May through September of 2004, but did not transmit the report to Congress until November of 2005, over a year after these trips were taken.

DHS has not provided sufficient resources to the Visa Waiver Program Oversight Unit to effectively monitor the risks posed by the visa waiver countries on an ongoing basis. While the unit developed a strategic plan to monitor the program, it is unable to fully implement the plan because it does not have enough staff and resources. In addition, DHS has not established Visa Waiver Program points of contact with U.S. embassies so that it can communicate directly with foreign government contacts and field officials who are best positioned to monitor compliance with the program's requirements and report on current events and issues of potential concern. Without this outreach, DHS is not able to leverage the existing resources at U.S. embassies in all visa waiver countries to obtain current information on potential risks, as well as the country's progress in addressing these risks.

Our report identifies a number of actions that DHS has taken to try to mitigate some of these risks. For example, they terminated the use of German temporary passports under the program when they learned that these documents were not well controlled.

In the interest of time, I am just going to quickly summarize our recommendations. We made several recommendations to the Department of Homeland Security to strengthen this program, including the creation of a real-time monitoring mechanism to improve communication between the Department and overseas posts; to improve additional resources for the Visa Waiver Program Unit so that they can conduct their mission. We also made a series of recommendations to mitigate the program's risks, including communicating clear operating standards for reporting lost and stolen passports. Finally, we recommended that the Congress consider establishing a deadline by which the Department must complete its biennial country assessments to provide more timely reporting to the Congress.

We believe these recommendations will help strengthen the program, and it is essential that the Department take strong actions—

Senator FEINSTEIN. Mr. Chairman, if I may, Mr. Ford, would you just repeat that last recommendation once again, please?

Mr. FORD. We recommended that the Congress consider establishing a deadline by which the Department would complete its biennial country assessments and report that information to Congress. And, again, that was to address the timeliness problem that we found with the last report they sent to you all. They sent it to you in November of 2005, but it was based on information collected in 2004, and a lot of that information was dated as well. So some of the information in the report you received was 2 to 3 years old. We think that Congress needs to have more up-to-date information so they have a better understanding of what the security risks are in these countries.

Senator FEINSTEIN. Thank you.

Mr. FORD. With that, I think I will close, and I would be happy to answer of your questions.

[The prepared statement of Mr. Ford appears as a submission for the record.]

Chairman KYL. Thanks very much. Like our previous witnesses, there is a lot to talk about. We do appreciate your succinctness and directness.

Mr. Laylagian?

STATEMENT OF LEON LAYLAGIAN, EXECUTIVE VICE PRESIDENT, PASSENGER-CARGO SECURITY GROUP, WASHINGTON, D.C.

Mr. LAYLAGIAN. Thank you, Chairman Kyl, Senator Feinstein. I thank you for the opportunity to be here today and provide testimony on—

Senator FEINSTEIN. Could you turn on your microphone, please? Just press that button.

Mr. LAYLAGIAN. Thank you for the opportunity to be here today to provide testimony on this most important issue of aviation security. My name is Leon Laylagian. I am the Executive Vice President of the Passenger-Cargo Security Group. PCSG, a trade association, working with legislators, regulators, and aviation security professionals, is dedicated to providing solutions in efforts to improve aviation security. PCSG has a professional partnership with over 22,000 airline pilots, an affiliation with nearly 400,000 airline passengers, and numerous industry leaders. I am also an airline pilot of 17 years with over 12,000 hours of flight time in a variety of aircraft, both domestically and international. I have flown for three passenger carriers and presently fly a Boeing 757 and 767 for a major all-cargo airline. My airline security work began in 1993, and I have served in many different capacities with unions and grass-roots efforts to improve airline security. I have served on various government working groups, including the TSA's Aviation Security Advisory Council for cargo security in 2003. I am also a graduate of Embry-Riddle Aeronautical University, also having served in the United States Navy.

The British police foiled the recent London airline bombing plot and, much like the 1995 Operation Bojinka, averted mass murder on an unimaginable scale. The human element, intelligence gathering, and its proper distribution carried the day in both cases. However, on a day-to-day operational scale, available technologies are necessary tools to add important layers of security.

As a working group member of the 2003 TSA Cargo ASAC, we waited a long time for rulemaking that falls short of reality. Placing the Known Shipper Program at the tip of our cargo security spear is not the answer. Other members of the ASAC hold the same discomfort with this approach, which seems to favor a perceived economic bias against technology application. In the U.S., a very small percentage of our belly-checked or loaded-in-belly-pits cargo undergo electronic or physical inspection. Some technology is transported around the country for use on a purely random basis, while a majority of the cargo relies on the Known Shipper Program, which we all know did nothing to prevent Charles McKinley from shipping himself from New York to Texas. Of course, this does not address the all-cargo airline, which is a tragic loophole.

On an international arena, many countries are using technologies to inspect significant portions of the belly freight loaded on passenger jets. The tools vary from high-energy X-ray and CT scan to spectral analysis, K–9s and sub-pressure simulation or altitude chambers.

Two countries in particular have a proven track record over the last 5 years using what is now old technology for mitigating smuggling, contraband, and terrorist-related shipments. No single layer is perfect, but the combined strength of the multiple layers will best deflect the terrorist vector.

Back to the Known Shipper Program, this has the potential to be a very valuable tool used to focus on which shipments require more scrutiny. Presently, the TSA has not required the development of a central database due to shipper concerns of proprietary information with respect to competitors. Instead of the green or red vetting of the program, we would recommend a more articulate program to include green, yellow, orange, and red to account for not only the origin and destination of the shipment, but also to address the supply chain. And those that handle packages in the chain should have a thorough and meaningful background check.

A 40-percent electronic inspection requirement should be in addition to this program, coupled with a random inspection feature which would make an enhanced Known Shipper Program a very useful tool.

As a final note on international operations, it would be of benefit to the American public if the TSA collaborated with our European counterparts and took advantage of their repeated offers to demonstrate to us how they employ technology effectively without damaging throughput or incurring a cost burden. Legislators such as Senator Feinstein have introduced language in the past to improve this segment of aviation security. While many of the technologies are not perfect, they are effective at mitigating threat. If we require spending on R&D for 2 years with implementation beginning 1 year following, we will embark on a process that will add a meaningful layer of security. The question is: Do we buy the computer today, or do we wait a few months for the improvements? The answer is: We need the tools now to get the job done and can ill afford doing nothing when we can be doing something to mitigate the threat.

I call on Congress to enact a law that will address the urgent need to inspect cargo instead of relying on the paperwork that only

addresses the chain of custody of a given shipment, and to provide the necessary funding to support this critical element of our National infrastructure.

Thank you again, Chairman Kyl, Senator Feinstein, and I welcome any questions you may have.

[The prepared statement of Mr. Laylagian appears as a submission for the record.]

Chairman KYL. Thank you very much. I just heard an official this morning taking the opposite side of the issue that you just articulated, but it is one of these great conundrums. You have technology that is available today that is not the best, but it is what we have. And you try to get it out into the field, and somebody says, "Well, but we have something just around the corner that is going to be a whole lot better. Why don't you wait?" Of course, it is more expensive. And it is always a very difficult proposition as to what you put your money in. And then you have the long-term research into something really, really great for things like nuclear weaponry. For example, we held a hearing on that in this Subcommittee that you will want to look into. So, I mean, there is no easy answer to that question, I appreciate.

Mr. Ford, you talked about the deadline on the visa waiver country assessments, and I just wonder: What is it that takes so long to get those done? Is it the lack of staff?

Mr. FORD. Well, we think that is part of the problem. We do not think that the Oversight Unit was adequately resourced in conducting the review. There were a number of interagency team members who were involved in the process. The site visits were taken in—I think it was from June to September of 2004. It took over a year for the reports to be drafted and cleared, and we know that the content of the report, which is classified contained a lot of outdated information. And there was other information that subsequently was available that was not in the report.

So we think for these reports to be useful to Congress, they should have as much current information in them as they possibly can. So that is one of the reasons we suggested that Congress may want to require that DHS, you know, speed the process up.

I might add that I mentioned that they reviewed 25 of the 27 countries. The other two countries that they did not get to, they began the review of that in the spring of 2005, and they still have not reported the results of those two countries to the Congress yet. So I am not so sure that they have been able to resolve the timeliness factor about getting this information quickly to the Hill.

Chairman KYL. I appreciate that. Could you just quickly tell me what you see as the security benefits of the new e-passport for visa waiver travelers?

Mr. FORD. I think the e-passport, because of the additional protections that it has in it, has the potential to ward off some of the risks from the old passports that can be more readily counterfeited or can be used—someone could take a blank passport that had been stolen and insert a photograph.

The new e-passports have the new technology which makes it much more difficult for them to be counterfeited. The concern that we have, though, is that many passports are good for 10 years, so even with the new e-passports, they may be good for the people

who get them now, but for those people who continue to have the old passports, or access to them, that is where the risk is. And until, you know, the old passport system is exhausted, we are going to have a potential security risk, in our view.

Chairman KYL. Thanks very much.

You all had to wait a long time, and then you sat through the first panel, and I said we would try to conclude this by 4 o'clock, so I am going to quickly move on to Senator Feinstein here.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Mr. Ford, I think your report is excellent, and I really thank you for it. I think you point out a number of things that are obvious and some that are not obvious, and clearly we should take some action.

You indicated that you felt that the Congress should take some action, and I would like to talk to Senator Kyl, and hopefully we will initiate something along the lines that you suggest.

I would ask you, Mr. Laylagian, about the cargo inspection. You say that a meaningful inspection formula would require 40 percent using electronic or physical means, 40 percent chosen by an enhanced Known Shipper Program. What is that?

Mr. LAYLAGIAN. Well, it would better refine or articulate the Known Shipper Program to cover not only—you have the 400,000 known shippers, but you have hundreds of thousands of handlers that would be involved in the movement of those shipments from the departure point to its arrival. And what the enhancement would be would be, in essence, a package profiling system should be collected in a central database, would be the best way for the TSA, I think, to manage that because they would have control over that information. And depending on the knowledge of where the departure point is, who the shippers are, who the ownership of those shippers are, and where it is going and how it is getting there, what hands are being put on that shipment on its way would better refine what type of technology application should be put on that.

Senator FEINSTEIN. So, in other words, you measure the shipment by those who touch it.

Mr. LAYLAGIAN. That would be a big part of it, and the content.

Senator FEINSTEIN. So if you get those who touch it well known, then you can find danger points, either with people who are not well known or people who may not be reliable shippers. Is that the point?

Mr. LAYLAGIAN. Yes, ma'am.

Senator FEINSTEIN. And then you would have the series of red, green, yellow, whatever the colors are, that would identify what the problem was.

Mr. LAYLAGIAN. What the vetting level of the handlers might be. I mean, right now the background check information is not to a level that it should be.

Senator FEINSTEIN. Do you think that is more effective than X-ray or K-9?

Mr. LAYLAGIAN. It is a tool; it is a layer. I mean, if you were trying to cover a hole in the ground and you had one pie plate to cover it, if it was a manhole, you would have a hard time preventing things from going through there. That is the Known Shipper Pro-

gram. You have got one pie plate over that hole. You add different types of technologies, they are not—none of them are perfect in their forms the way they are right now, but they do a reasonable job of getting that job done. You add two, three, four pie plates, you start mitigating, you start adding the layers to cover that hole and protect it. You are never going to make anything perfect, but right now essentially we are—

Senator FEINSTEIN. Well, let me ask you a question. This would be applied to all airports or major airports?

Mr. LAYLAGIAN. It could be applied across the system, and it could be done effectively across the system, and it could be done on a risk assessment basis as to which airports you would choose to cover or not. There are some small airports that do not have the infrastructure or logistics to manage certain types of electronic inspection equipment. Portable systems might be effective for them during seasonal portions of the course of the year. But it may not be that way, in which case you would be able to make those decisions with the more refined Known Shipper Program, making that a better tool to make that call.

Senator FEINSTEIN. Has this been discussed with TSA?

Mr. LAYLAGIAN. It has. It has certainly been discussed during the ASAC. There is an ongoing discussion right now. There is the freight assessment system, which has turned into the Cargo Working Group. It is a continuing conversation as to how they work those details out.

There is a lot of resistance to setting up a central database, which I think is problematic for the Known Shipper Program. There are certain things that are hindering the effectiveness of the Known Shipper Program right now, and rather than just making it a good or bad proposition, my recommendation to make it more articulate by adding four steps rather than two, would be better able to decide which shipments should receive more scrutiny—shipments of sweatshirts, high-energy X-ray, I mean, there are certain things that you should not be seeing in that shipment, and that would be a way of deciding how that tool could be better used.

Senator FEINSTEIN. Okay. Well, thank you. If you have any other—I appreciate your writing here, but if you have any other specific recommendations of what we might do, I think we would both appreciate receiving them.

Mr. LAYLAGIAN. There are a number of aviation security professionals and even managers that work in the cargo arena for passenger carriers. If I can collect them and sit down together with you, I think we clearly could make recommendations.

Senator FEINSTEIN. Thank you. If you would do that, that would be appreciated.

Mr. LAYLAGIAN. Yes, Senator.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman KYL. Thank you very much, and I want to thank this panel as well. Mr. Ford, we know where to get you, and we will probably be in touch with you from time to time, but we appreciate the report that you issued here, and your testimony as well. And, likewise, Mr. Laylagian, if you can get some recommendations to us from other folks, that would be appreciated, too.

We will leave the record open—I don't know how many days, but a few days—for other members to submit questions to you and for you to submit anything else that you think would be useful to us. We appreciate your testimony very much, and if there is nothing else, then I will adjourn this meeting of the Subcommittee. It is adjourned.

[Whereupon, at 4:00 p.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

[Additional material is being retained in the Committee files.]

SUBMISSIONS FOR THE RECORD

United States Government Accountability Office

GAO

Testimony

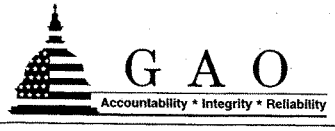
Before the Subcommittee on Terrorism, Technology, and Homeland Security, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 2:00 p.m. EDT
Thursday, September 7, 2006

BORDER SECURITY

Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program

Statement of Jess T. Ford, Director
International Affairs and Trade



GAO-06-1090T

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

September 7, 2006

GAO
Accountability Integrity Reliability

Highlights

Highlights of GAO-06-1090T, a testimony before the Chairman, Subcommittee on Terrorism, Technology, and Homeland Security, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

The Visa Waiver Program enables citizens of 27 countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. In fiscal year 2005, nearly 16 million people entered the country under the program. After the 9-11 terrorist attacks, the risk that aliens would exploit the program to enter the United States became more of a concern. This testimony discusses our recent report on the Visa Waiver Program. Specifically, it (1) describes the Visa Waiver Program's benefits and risks, (2) examines the U.S. government's process for assessing potential risks, and (3) assesses the actions taken to mitigate these risks. We met with U.S. embassy officials in six program countries and reviewed relevant procedures and reports on participating countries.

What GAO Recommends

In our report, we made a series of recommendations to DHS to strengthen its ability to assess and mitigate the program's risks, such as providing more resources to the program's monitoring unit and issuing standards for the reporting of lost and stolen passport data. We also stated that Congress should consider establishing a deadline for the mandated biennial report to Congress. DHS generally agreed with our report and recommendations, but did not agree that Congress should establish a deadline for the biennial report.

www.gao.gov/cgi-bin/getrpt?GAO-06-1090T

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jess Ford at (202) 512-4128 or fordj@gao.gov.

BORDER SECURITY

Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program

What GAO Found

The Visa Waiver Program has many benefits as well as some inherent risks. It facilitates travel for millions of people and eases consular workload, but poses challenges to border inspectors, who, when screening visa waiver travelers, may face language barriers or lack time to conduct in-depth interviews. Furthermore, stolen passports from visa waiver countries are prized travel documents among terrorists, criminals, and immigration law violators, creating an additional risk. While the Department of Homeland Security (DHS) has intercepted many fraudulent documents at U.S. ports of entry, DHS officials acknowledged that an undetermined number of inadmissible aliens may have entered the United States using a stolen or lost passport from a visa waiver country.

DHS's process for assessing the risks of the Visa Waiver Program has weaknesses. In 2002, Congress mandated that, every 2 years, DHS review the effect that each country's continued participation in the program has on U.S. law enforcement and security interests, but did not set a reporting deadline. In 2004, DHS established a unit to oversee the program and conduct these reviews. We identified several problems with the 2004 review process, as key stakeholders were not consulted during portions of the process, the review process lacked clear criteria and guidance to make key judgments, and the final reports were untimely. Furthermore, the monitoring unit cannot effectively achieve its mission to monitor and report on ongoing law enforcement and security concerns in visa waiver countries due to insufficient resources.

DHS has taken some actions to mitigate the program's risks; however, the department has faced difficulties in further mitigating these risks. In particular, the department has not established time frames and operating procedures regarding timely stolen passport reporting—a program requirement since 2002. Furthermore, DHS has sought to require the reporting of lost and stolen passport data to the United States and the International Criminal Police Organization (Interpol), but it has not issued clear reporting guidelines to participating countries. While most visa waiver countries report to Interpol's database, four do not. Further, DHS is not using Interpol's data to its full potential as a border screening tool because U.S. border inspectors do not automatically access the data at primary inspection.

September 7, 2006

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here to discuss our observations on the Visa Waiver Program. In fiscal year 2005, nearly 16 million travelers entered the United States under this program, which facilitates international travel and commerce, and eases workload for consular officers at overseas posts, by enabling citizens of 27 participating countries[1] to travel to the United States for tourism or business for 90 days or less without first obtaining a visa.[2] Participating countries were selected because their citizens had demonstrated a pattern of compliance with U.S. immigration laws, and the governments of these countries granted reciprocal visa-free travel to U.S. citizens. The Visa Waiver Program was created as a pilot program in 1986,[3] and it became permanent in 2000,[4] about 1 year prior to the 9-11 terrorist attacks. After the attacks, the potential risks of the program became more of a concern. In particular, convicted terrorist Zacarias Moussaoui and "shoe-bomber" Richard Reid both boarded flights to the United States with passports issued by Visa Waiver Program countries. Moreover, the foiled alleged terrorist plot to board planes at London's Heathrow Airport and fly to the United States with explosive materials highlights the importance of having effective tools to ensure that only legitimate travelers enter the United States. In May 2002, Congress mandated that the Department of Homeland Security (DHS) evaluate and report to Congress at least every two years on the effect that each country's continued participation in the program has on

[1]The participating countries are Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

[2]The United States also issues visas to those who intend to immigrate to the United States. In this testimony, we use the term "visa" to refer to nonimmigrant visas only.

[3]The Immigration Reform and Control Act of 1986, P.L. 99-603.

[4]The Visa Waiver Permanent Program Act, P.L. 106-396.

U.S. law enforcement and security interests.[5] Effective oversight of the Visa Waiver Program is essential to find the right balance between facilitating legitimate travel and preventing potential terrorists, criminals, and others that may pose law enforcement and immigration concerns from entering the United States.[6]

Earlier this week, we released two reports on the Visa Waiver Program: the first discusses the process by which the United States assesses and mitigates the program's risks,[7] and the second describes the process by which additional countries may be admitted into the program.[8] My statement will focus on the first of these reports. Specifically, I will discuss (1) the Visa Waiver Program's advantages and potential risks; (2) the U.S. government's process for assessing the program's risks; and (3) the actions that have been taken to mitigate these risks. In addition, we have ongoing work examining international aviation passenger prescreening, including DHS's use of passport and reservation data to screen travelers and the pilot Immigration Advisory Program at several airports overseas, and expect to report on our findings later this fall.

In conducting this work, we reviewed documentation, including the laws governing the program, relevant regulations and agency operating procedures, and DHS's Office of the Inspector General (OIG) reports. We also examined 15 of the 25 completed reports from the 2004 review process that assessed the participation of Visa Waiver Program

---

[5]Prior to this change, DHS was required to report at least once every 5 years. See the Enhanced Border Security and Visa Entry Reform Act, P.L 107-173.

[6]Since September 11, 2001, the visa issuance process has taken on greater significance as an antiterrorism tool, as we have previously reported. GAO has issued a series of reports on the visa issuance process. See GAO, *Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, GAO-05-859 (Washington, D.C.: Sept. 13, 2005); *Border Security: Actions Needed to Strengthen Management of Department of Homeland Security's Visa Security Program*, GAO-05-801 (Washington, D.C.: July 29, 2005); and, *Border Security: Visa Process Should be Strengthened as an Antiterrorism Tool*, GAO-03-132NI (Washington, D.C.: Oct. 21, 2002).

[7]GAO, *Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*, GAO-06-844 (Washington, D.C.: July 28, 2006).

[8]GAO, *Process for Admitting Additional Countries into the Visa Waiver Program*, GAO-06-835R (Washington, D.C.: July 28, 2006).

countries.[9] Additionally, we interviewed political, economic, consular, commercial, and law enforcement officials at U.S. embassies in six Visa Waiver Program countries, as well as foreign government officials in three of these countries. We met with officials from several DHS component agencies and offices; the Department of State (State); and the International Criminal Police Organization (Interpol) in Lyon, France. We conducted our work in accordance with generally accepted government auditing standards (see app. I for a list of related GAO products and ongoing reviews).

Summary

The Visa Waiver Program provides many benefits to the United States, including facilitating international travel for millions of foreign citizens seeking to visit the United States each year, creating substantial economic benefits to our country. Visa waiver travelers have represented about one-half of all nonimmigrant admissions to the United States in recent years. The program also allows State to allocate resources to visa-issuing posts in countries with higher-risk applicant pools. Moreover, participating visa waiver countries offer visa-free travel to U.S. citizens. However, travelers visiting the United States under the Visa Waiver Program can pose potential security risks because they are not interviewed by a consular officer prior to their travel. In addition, border inspectors at U.S. ports of entry may not know the visa waiver traveler's language or local fraudulent document trends in the traveler's home country, nor have the time to conduct an extensive interview. In contrast, visa-issuing officers at U.S. embassies generally have more time to interview applicants—often in the applicants' native language—and have more country-specific knowledge of passports and fraud trends. Furthermore, lost and stolen passports from visa waiver countries are highly prized among travelers seeking to conceal their true identities or nationalities, increasing the likelihood that terrorists and other criminals would attempt to obtain these documents. DHS officials have acknowledged that an undetermined number of inadmissible aliens may have entered the United States using a stolen or lost passport from a visa waiver country. In fact,

[9]As of June 2006, the remaining 10 assessments were pending classification review, and assessments of the remaining two participating countries—Italy and Portugal—were in process.

passports from Visa Waiver Program countries have been used illegally by hundreds of travelers attempting to enter the United States. For example, from January through June 2005, at U.S. ports of entry, DHS confiscated 298 passports issued by Visa Waiver Program countries that travelers were attempting to use fraudulently for admission into the United States. Thus, there is a risk that the program could be exploited for illegal entry into the United States.

DHS has developed a process for assessing the law enforcement and security risks of the Visa Waiver Program, but this process has weaknesses. In 2002, Congress mandated that DHS review the security risks posed by each visa waiver country's participation in the program at least every 2 years. In 2004, DHS established the Visa Waiver Program Oversight Unit within the Office of International Enforcement (OIE).[10] DHS conducted its first mandated biennial reviews that same year, and subsequently determined that all of the countries it reviewed should remain in the program.[11] However, we identified several problems with the country review process. Specifically, key interagency stakeholders,[12] such as embassies overseas and forensic document analysts, were left out of portions of the 2004 country review process, and the review process lacked clear criteria and guidance to make key judgments. Also, the country assessments prepared by DHS were not completed in a timely fashion and contained some dated information that did not necessarily reflect current risks; interagency teams conducted site visits as part of the country assessments from May through September 2004, and transmitted the final report to Congress more than 1 year later, in November 2005. The teams collecting information about the visa waiver countries' risks in 2004 used, in some cases, information that was

[10]OIE is located in the Office of Policy Development under the direction of the Assistant Secretary of Homeland Security for Policy.

[11]DHS's Office of Policy began this review in early 2004, several months before the Visa Waiver Program Oversight Unit was established in July of that year.

[12]The interagency working group charged in 2004 with assessing participating countries' adherence to the program's statutory requirements comprised officials from Justice's Office of International Affairs, State's Bureau of Consular Affairs, and several components within DHS, including the Intelligence and Analysis Directorate, Custom and Border Protection's Office of Field Operations, and Immigration and Customs Enforcement's Forensic Document Laboratory, among others. Representatives from some of these agencies formed the in-country site visit teams.

two years old; by the time the summary report was issued in November 2005, some of the data was over 3 years old. Moreover, DHS has not provided sufficient resources to the Office of International Enforcement to effectively monitor the risks posed by visa waiver countries on an ongoing basis. While the Visa Waiver Program Oversight Unit developed a strategic plan to monitor the program, it has been unable to implement this plan with its current staff of only two full-time employees. In addition, DHS has not established Visa Waiver Program points of contact within the U.S. embassies so it can communicate directly with foreign government contacts and field officials, who are best positioned to monitor compliance with the program's requirements and report on current events and issues of potential concern. Without this outreach, DHS is not able to leverage the existing resources at U.S. embassies in all visa waiver countries to obtain current information on potential risks, as well as countries' progress in addressing these risks.

DHS has taken some actions to mitigate the risks of the Visa Waiver Program. Specifically, DHS identified security concerns in several participating countries during the 2004 assessment process, and, for example, terminated the use of the German temporary passport under the program. However, the department has faced difficulties in further mitigating program risks, particularly regarding lost and stolen passport reporting—a key vulnerability. For example, not all countries have consistently reported their data to the United States on stolen blank passports, even though reporting such data is vital to mitigating program risks. In one instance, a visa waiver country reported to the United States the theft of nearly 300 blank passports more than 9 years after the theft occurred. In 2002, timely reporting of such thefts became a statutory requirement for continued participation in the program, but DHS has not issued standard operating procedures for countries to report these data. DHS has also sought to expand this requirement to include the reporting of data, to the United States and Interpol,[13] about

[13]Interpol is the world's largest international police organization, with 184 member countries. Created in 1923, it facilitates cross-border police cooperation, and supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime. In July 2002, Interpol established a database on lost and stolen travel documents. As of June 2006, the database contained about 11.6 million records of lost and stolen passports.

lost and stolen issued[14] (as well as blank) passports; however, the United States lacks a centralized mechanism for foreign governments to report all stolen passports, and DHS has not identified the U.S. government entity to which participating countries should report this information. While most visa waiver countries contribute to Interpol's database, four do not. Moreover, some countries that do contribute do not do so on a regular basis, according to Interpol officials. In addition, Interpol's data on lost and stolen travel documents is not automatically accessible to U.S. border inspectors at primary inspection—one reason why it is not an effective border screening tool, according to DHS, State, and Justice officials. According to the Secretary General of Interpol, until DHS can automatically query Interpol's data, the United States will not have an effective screening tool for checking passports. However, DHS has not yet finalized a plan to obtain this systematic access to Interpol's data.

In our report, we made several recommendations to DHS to strengthen its ability to assess the risks of the Visa Waiver Program, including a recommendation to create real-time monitoring mechanisms to improve communication between the department and overseas posts, and to provide additional resources for the Visa Waiver Program Oversight Unit. We also made a series of recommendations to mitigate the program's risks, including communicating clear standard operating procedures for the reporting of lost and stolen, blank and issued, passport data. Finally, we included a matter for congressional consideration: to improve the timeliness of DHS's assessments of the risks of each country's continued participation in the program, Congress should consider establishing a deadline by which the department must complete its biennial country assessments and report to Congress. DHS either agreed with, or stated that it is considering, all of our recommendations. Regarding our matter for congressional consideration, DHS did not support the establishment of a deadline for the biennial report to Congress. Instead, DHS suggested that Congress should require continuous and ongoing evaluation of the risks of each country's continued participation in the program.

[14]Issued passports have been officially personalized with the bearer's biographical information.

Background

The Immigration Reform and Control Act of 1986 created the Visa Waiver Program as a pilot program.[15] It was initially envisioned as an immigration control and economic promotion program, according to State. Participating countries were selected because their citizens had a demonstrated pattern of compliance with U.S. immigration laws, and the governments of these countries granted reciprocal visa-free travel to U.S. citizens. In recent years, visa waiver travelers have represented about one-half of all nonimmigrant admissions to the United States. In 2002, we reported on the legislative requirements to which countries must adhere before they are eligible for inclusion in the Visa Waiver Program.[16] In general, to qualify for visa waiver status, a country must:

- maintain a nonimmigrant refusal rate of less than 3 percent for its citizens who apply for business and tourism visas.
- certify that it issues machine-readable passports to its citizens; and
- offer visa-free travel for U.S. citizens.

Following the 9-11 attacks, Congress passed additional laws to strengthen border security policies and procedures, and DHS and State instituted other policy changes that have affected the qualifications for countries to participate in the Visa Waiver Program. For example, all passports issued after October 26, 2005, must contain a digital photograph printed in the document, and passports issued to visa waiver travelers after October 26, 2006, must be electronic (e-passports).[17] In addition, the May 2002 Enhanced

[15]P.L. 99-603.

[16]See GAO, *Border Security: Implications of Eliminating the Visa Waiver Program*, GAO-03-38 (Washington, D.C.: Nov. 22, 2002).

[17]Travelers with passports issued after the deadline that do not meet these requirements must obtain a visa from a U.S. embassy or consulate overseas before departing for the United States. In general, e-passports will contain a chip embedded in the passport that will store the same information that is printed on the data page of the passport, such as name, date of birth, gender, place of birth, dates of passport issuance and expiration, place of issuance, passport number, and a photo image of the bearer.

Border Security and Visa Reform Act required that participating countries certify that the theft of their blank passports is reported to the U.S. government in a timely manner.

Visa Waiver Program Has Benefits and Risks

The Visa Waiver Program has many benefits. The program was created to facilitate international travel without jeopardizing the welfare or security of the United States, according to the program's legislative history. According to economic and commercial officers at several of the U.S. embassies we visited, visa-free travel to the United States boosts international business travel and tourism, as well as airline revenues, and creates substantial economic benefits to the United States. Moreover, the program allows State to allocate its resources to visa-issuing posts in countries with higher-risk applicant pools. In 2002, we reported that eliminating the program would increase State's resource requirements as millions of visa waiver travelers who have benefited from visa-free travel would need to obtain a visa to travel to the United States if the program did not exist.[18] Specifically, if the program were eliminated, we estimated that State's initial costs at that time to process the additional workload would likely range between $739 million and $1.28 billion and that annual recurring costs would likely range between $522 million and $810 million. In addition, visa waiver countries could begin requiring visas for U.S. citizens traveling to the 27 participating countries for temporary business or tourism purposes, which would impose a burden of additional cost and time on U.S. travelers to these countries.

Visa Waiver Program Can Pose Risks to U.S. Security, Law Enforcement, and Immigration Interests

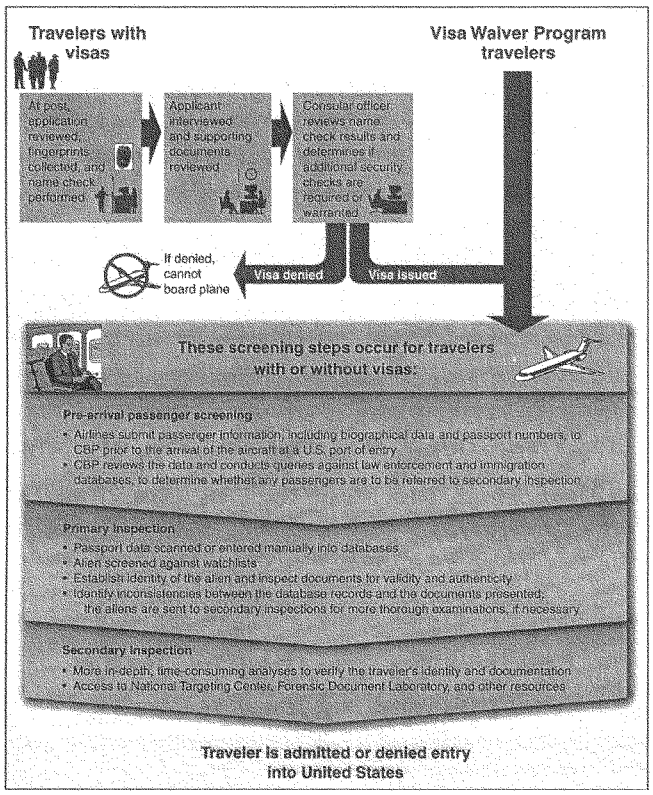
The Visa Waiver Program, however, can also pose risks to U.S. security, law enforcement, and immigration interests because some foreign citizens may exploit the program to enter the United States. First, visa waiver travelers are not subject to the same degree of screening as travelers who must first obtain a visa before arriving in the United States (see fig. 1). Visa waiver travelers are first screened in person by a DHS

[18]GAO-03-38.

Customs and Border Protection (CBP) inspector once they arrive at the U.S. port of entry, perhaps after having already boarded an international flight bound for the United States with a fraudulent travel document. According to the DHS OIG, primary border inspectors are at a disadvantage when screening Visa Waiver Program travelers because they may not know the alien's language or local fraud trends in the alien's home country, nor have the time to conduct an extensive interview. In contrast, non-visa-waiver travelers, who must obtain a visa from a U.S. embassy or consulate, receive two levels of screening before entering the country—in addition to the inspection at the U.S. port of entry, these travelers undergo an interview by consular officials overseas, who conduct a rigorous screening process when deciding to approve or deny a visa. As we have previously reported, State has taken a number of actions since 2002 to strengthen the visa issuance process as a border security tool.[19] Moreover, consular officers have more time to interview applicants and examine the authenticity of their passports, and may also speak the visa applicant's native language, according to consular officials. Therefore, inadmissible travelers who need visas to enter the United States may attempt to acquire a passport from a Visa Waiver Program country to avoid the visa screening process.

[19]GAO-05-859 and GAO-03-132NI.

Figure 1: Comparison of Screening for U.S. Visas versus Arrival Inspection Screening at U.S. Air Port of Entry



Sources GAO; Nova Development (clip art)

Another risk inherent in the program is the potential exploitation by terrorists, immigration law violators, and other criminals of a visa waiver country's lost or stolen passports. DHS intelligence analysts, law enforcement officials, and forensic document experts all acknowledge that misuse of lost and stolen passports is the greatest security problem posed by the Visa Waiver Program. Lost and stolen passports from visa waiver countries are highly prized travel documents, according to the Secretary General of

Interpol. Moreover, Visa Waiver Program countries that do not consistently report the losses or thefts of their citizens' passports, or of blank passports, put the United States at greater risk of allowing inadmissible travelers to enter the country.

Fraudulent passports from Visa Waiver Program countries have been used illegally by travelers seeking to disguise their true identities or nationalities when attempting to enter the United States. For example, from January through June 2005, DHS reported that it confiscated, at U.S. ports of entry, 298 fraudulent or altered passports issued by Visa Waiver Program countries that travelers were attempting to use for admission into the United States. Although DHS has intercepted some travelers with fraudulent passports at U.S. ports of entry, DHS officials acknowledged that an undetermined number of inadmissible aliens may have entered the United States using a lost or stolen passport from a visa waiver country. According to State, these aliens may have been inadmissible because they were immigration law violators, criminals, or terrorists. For example:

- In July 2005, two aliens successfully entered the United States using lost or stolen Austrian passports. DHS was not notified that these passports had been lost or stolen prior to this date; the aliens were admitted, and there is no record of their departure, according to CBP. In October 2005, CBP referred this case to DHS's Immigration and Customs Enforcement for further action.

- In June 2005, CBP inspectors admitted into the United States two aliens using Italian passports that were from a batch of stolen passports. CBP was notified that this batch was stolen; however, the aliens altered the passport numbers to avoid detection by CBP officers. DHS has no record that these individuals departed the United States.

Process for Assessing Program Risks Has Weaknesses

DHS has taken several steps to assess the risks of the Visa Waiver Program. However, we identified problems with the country review process by which DHS assesses these risks, namely a lack of inclusiveness, transparency, and timeliness. Furthermore, OIE is unable to effectively monitor the immigration, law enforcement, and security risks posed by visa waiver countries on a continuing basis because of insufficient resources.

Initial Steps Taken To Assess Risk of Visa Waiver Program

In April 2004, the DHS OIG identified significant areas where DHS needed to strengthen and improve its management of the Visa Waiver Program. For example, the OIG found that a lack of funding, trained personnel, and other issues left DHS unable to comply with the mandated biennial country assessments. In response to these findings, DHS established OIE's Visa Waiver Program Oversight Unit in July 2004, and named a director to manage the office. The unit's mission is to oversee Visa Waiver Program activities and monitor countries' adherence to the program's statutory requirements, ensuring that the United States is protected from those who wish to do it harm or violate its laws, including immigration laws. Since the unit's establishment, DHS, and particularly OIE, has made strides to address concerns raised by the 2004 OIG review. For example, DHS completed comprehensive assessments of 25 of the 27 participating countries and submitted a six-page report to Congress in November 2005 that summarized the findings from the 2004 assessments.

DHS Lacks a Clearly-Defined, Consistent, and Timely Process to Assess Risks of Visa Waiver Program

Despite these steps to strengthen and improve the management of the program, we identified several problems with the mandated biennial country assessment process, by which DHS assesses the risks posed by each of the visa waiver countries' continued participation in the program. For the 2004 assessments, we found the following:

- *Some key stakeholders were excluded from the process.* After conducting the site visits and contributing to the reports on the site visits, DHS and the interagency working group did not seek input from all site visit team members while drafting and clearing the final country assessments and subsequent report to Congress. For example, DHS's forensic document analysts, who participated in the site visits in 2004, told us that they did not see, clear, or comment on the draft country assessments, despite repeated attempts to obtain copies of them. Additionally, at the time of our visits, ambassadors or deputy chiefs of mission in each of the six posts told us that they were not fully aware of the extent to which assessments for the country where they were posted discussed law enforcement and security concerns posed by the continued participation of the country in the program. Without this information, key stakeholders could not be effective advocates for U.S. concerns.

- *The reviews lacked clear criteria to make key judgments.* We found that DHS did not have clear criteria to determine at what point security concerns uncovered during their review would trigger discussions with foreign governments about these concerns and an attempt to resolve them. State officials agreed that qualitative and/or quantitative criteria would be useful when making these determinations, although DHS stated that the criteria should be flexible.

- *DHS and its interagency partners neither completed the 25 country assessments nor issued the summary report to Congress in a timely manner.* The interagency teams conducted site visits as part of the country assessments from May through September 2004, and transmitted the final summary report to Congress more than 1 year later, in November 2005. OIE, State, and Justice officials acknowledged that the assessments took too long to complete. The teams collecting information about the visa waiver countries' risks in 2004 used, in some cases, information that was two years old; by the time the summary report was issued in November 2005, some of the data was over 3 years old. As a result of this lengthy process, the final report presented to Congress did not necessarily reflect the current law

enforcement and security risks posed by each country, or the positive steps that countries had made to address these risks.

DHS Cannot Effectively Monitor Ongoing Concerns in Visa Waiver Countries

OIE is limited in its ability to achieve its mission because of insufficient staffing. The office has numerous responsibilities, including conducting the mandated biennial country reviews; monitoring law enforcement, security, and immigration concerns in visa waiver countries on an ongoing basis; and working with countries seeking to become members of the Visa Waiver Program. In 2004, the DHS OIG found that OIE's lack of resources directly undercut its ability to assess a security problem inherent in the program—lost and stolen passports. The office received funding to conduct the country reviews in 2004 and 2005; however, OIE officials indicated that a lack of funding and full-time staff has made it extremely difficult to conduct additional overseas fieldwork, as well as track ongoing issues of concern in the 27 visa waiver countries—a key limitation in DHS's ability to assess and mitigate the program's risks. According to OIE officials, the unit developed a strategic plan to monitor the program, but has been unable to implement its plan with its current staffing of two full-time employees, as well as one temporary employee from another DHS component. Without adequate resources, OIE is unable to monitor and assess participating countries' compliance with the Visa Waiver Program's statutory requirements.

In addition to resource constraints, DHS has not clearly communicated its mission to stakeholders at overseas posts, nor identified points of contact within U.S. embassies, so it can communicate directly with field officials positioned to monitor countries' compliance with Visa Waiver Program requirements and report on current events and issues of potential concern. In particular, within DHS's various components, we found that OIE is largely an unknown entity and, therefore, is unable to leverage the expertise of DHS officials overseas. A senior DHS representative at one post showed us that her organizational directory did not contain contact information for OIE. Additionally, a senior DHS official in Washington, D.C., told us that he may find out about developments—either routine or emergent—in visa waiver countries by "happenstance."

Due to the lack of outreach and clear communication about its mission, OIE is limited in its ability to monitor the day-to-day law enforcement and security concerns posed by the Visa Waiver Program, and the U.S. government is limited in its ability to influence visa waiver countries' progress in meeting requirements.

DHS Faces Difficulties in Mitigating Program Risks

DHS has taken some actions to mitigate the risks of the Visa Waiver Program. However, though the law has required the timely reporting of blank passport thefts for continued participation in the Visa Waiver Program since 2002, DHS has not established and communicated time frames and operating procedures to participating countries. In addition, DHS has sought to expand this requirement to include the reporting of data, to the United States and Interpol, on lost and stolen issued passports; however, participating countries are resisting these requirements, and DHS has not yet issued guidance on what information must be shared, with whom, and within what time frame. Furthermore, U.S. border inspectors are unable to automatically access Interpol's data on reported lost and stolen passports, which makes detection of these documents at U.S. ports of entry more difficult.

DHS Has Taken Some Actions to Mitigate Risks of the Visa Waiver Program

As previously mentioned, during the 2004 assessment process, the working group identified security concerns in several participating countries, and DHS took actions to mitigate some of these risks. Specifically, DHS determined that several thousand blank German temporary passports[20] had been lost or stolen, and that Germany had not reported some of this information to the United States. As a result, as of May 1, 2006, German temporary passport holders are not allowed to travel to the United States under the Visa Waiver Program without a visa. In addition, DHS has enforced an October 26,

[20]German temporary passports are valid for one year, and are less expensive than standard German passports. In addition, they are issued at more than 6,000 locations across Germany, whereas the Ministry of Interior issues the standard passports centrally.

2005, deadline requiring travelers under the Visa Waiver Program to have digital photographs in their passports.

DHS Lacks Standard Procedures for Obtaining Stolen Blank Passport Data

A key risk in the Visa Waiver Program is stolen blank passports from visa waiver countries, because detecting these passports at U.S. ports of entry is extremely difficult, according to DHS. Some thefts of blank passports have not been reported to the United States until years after the fact, according to DHS intelligence reports. For example, in 2004, a visa waiver country reported the theft of nearly 300 stolen blank passports to the United States more than 9 years after the theft occurred. The 2002 Enhanced Security and Visa Entry Reform Act provides that the Secretary of Homeland Security must terminate a country from the Visa Waiver Program if he and the Secretary of State jointly determine that the country is not reporting the theft of its blank passports to the United States on a timely basis. However, DHS has not established time frames or operating procedures to enforce this requirement. While the statute requires visa waiver countries to certify that they report information on the theft of their blank passports to the United States on a timely basis, as of June 2006, DHS has not defined what constitutes "timely" reporting. Moreover, the United States lacks a centralized mechanism for foreign governments to report all stolen passports. In particular, DHS has not defined to whom in the U.S. government participating countries should report this information.

Some Participating Visa Waiver Program Countries are Resisting Additional Reporting to United States and Interpol

In addition to blank passports, lost or stolen issued passports also pose a risk because they can be altered. In June 2005, DHS issued guidance to participating Visa Waiver Program countries requiring that they certify their intent to report lost and stolen passport data on issued passports by August 2005. However, DHS has not yet issued guidance on what information must be shared, with whom, and within what time frame. Moreover, some visa waiver countries have not yet agreed to provide this information to the United States, due in part to concerns over the privacy of their citizens' biographical

information. In addition, several consular officials expressed confusion about the current and impending requirements about sharing this data, and felt they were unable to adequately explain the requirements to their foreign counterparts.

In June 2005, the U.S. government also announced its intention to require visa waiver countries to certify their intent to report information on both lost and stolen blank and issued passports to Interpol. In 2002, Interpol developed a database of lost and stolen travel documents to which its member countries may contribute on a voluntary basis. While most visa waiver countries use and contribute to Interpol's database, four do not. Moreover, some countries that do contribute do not do so on a regular basis, according to Interpol officials. Participating countries have expressed concerns about reporting this information, citing privacy issues; however, Interpol's database on lost and stolen travel documents does not include the passport bearers' biographical information, such as name and date of birth.[21] According to the Secretary General of Interpol, in light of the high value associated with passports from visa waiver countries, it is a priority for his agency to encourage countries to contribute regularly to the database.

Inefficient Access to Interpol's Database on Lost and Stolen Passports

Though information from Interpol's database could potentially stop inadmissible travelers from entering the United States, CBP's border inspectors do not have automatic access to the database at the primary inspection point at U.S. ports of entry—the first line of defense against those who might exploit the Visa Waiver Program to enter the United States. The inspection process at U.S. ports of entry can include two stages—a primary and secondary inspection. If, during the primary inspection, the inspector suspects that the traveler is inadmissible either because of a fraudulent passport or other reason, the inspector refers the traveler to secondary inspection. At secondary inspection, border inspectors can contact officials at the National Targeting Center, who can query Interpol's stolen-travel-document database to determine if the traveler's

[21]Interpol's database includes the passport's identity number, the country of issuance, and the country where the loss or theft occurred. According to officials from Justice's Interpol-U.S. National Central Bureau, it is particularly important that countries report this information, as well as the date of the theft and the issuance date.

passport had been previously reported lost or stolen, but is not yet on CBP's watch list.[22] However, according to DHS, State, and Justice officials, because Interpol's data on lost and stolen travel documents is not automatically accessible to border inspectors at primary inspection, it is not currently an effective border screening tool. Moreover, according to the Secretary General of Interpol, until DHS can automatically query Interpol's data, the United States will not have an effective screening tool for checking passports. According to Interpol officials, the United States is working actively with Interpol on a potential pilot project that would allow for an automatic query of aliens' passport data against Interpol's database at primary inspection at U.S. ports of entry. However, DHS has not yet finalized a plan to do so.

Recommendations to Improve Program Oversight and DHS's Response

In our report, we made a series of recommendations to improve the U.S. government's process for assessing the risks in the Visa Waiver Program, including recommending that DHS provide additional resources to strengthen OIE's visa waiver monitoring unit; finalize clear, consistent, and transparent protocols for the biennial country assessments and provide these protocols to stakeholders at relevant agencies at headquarters and overseas; create real-time monitoring arrangements for all 27 participating countries; and establish protocols for direct communication between overseas posts and OIE's Visa Waiver Program Oversight Unit. In addition, we made recommendations to improve U.S. efforts to mitigate program risks, including requiring that all visa waiver countries provide the United States and Interpol with non-biographical data from lost or stolen issued passports, as well as from blank passports; developing clear standard operating procedures for the reporting of lost and stolen blank and issued passport data; and developing and implementing a plan to make Interpol's stolen travel document database automatically available during primary inspection at U.S. ports of entry. Given the lengthy time it took for DHS to issue the November 2005 summary report to Congress,

[22]Interpol's data on lost and stolen passports are not available when border inspectors screen travelers' passports at primary inspection unless Interpol has shared this information with the United States in separate reports and it has been manually entered into DHS watch lists.

and to ensure future reports contain timely information when issued, we also proposed that Congress establish a biennial deadline by which DHS must complete the country assessments and report to Congress.

DHS either agreed with, or stated that it is considering, all of our recommendations. Regarding our matter for congressional consideration, DHS did not support the establishment of a deadline for the biennial report to Congress. Instead, DHS suggested that Congress should require continuous and ongoing evaluation. With continuous review, DHS stated that it would be able to constantly evaluate U.S. interests and report to Congress on the current 2-year reporting cycle on targeted issues of concern, rather than providing a historical evaluation. We agree that continuous and ongoing evaluation is necessary, and that is why we recommended that DHS create real-time monitoring arrangements and provide additional resources to the Visa Waiver Program Oversight Unit to achieve this goal. Regarding the mandated biennial country assessments, we believe that they can serve a useful purpose if they are completed in a timely fashion.

In closing, the Visa Waiver Program aims to facilitate international travel for millions of people each year and promote the effective use of government resources. Effective oversight of the program entails balancing these benefits against the program's potential risks. To find this balance, the U.S. government needs to fully identify the vulnerabilities posed by visa waiver travelers, and be in a position to mitigate them. It is imperative that DHS commit to strengthen its ability to promptly identify and mitigate risks to ensure that the Visa Waiver Program does not jeopardize U.S. security interests. This is particularly important given that many countries are actively seeking to join the program.

Mr. Chairman, this concludes my prepared statement. I will be happy to answer any questions you or Members of the Subcommittee may have.

Contacts and Staff Acknowledgments

For questions regarding this testimony, please call Jess T. Ford, (202) 512-4128 or fordj@gao.gov. Individuals making key contributions to this statement include John Brummet, Assistant Director, and Kathryn H. Bernet, Joseph Carney, and Jane S. Kim.

Appendix I: Related GAO Products and Ongoing Reviews

Issued Reports

Border Security: More Emphasis on State's Consular Safeguards Could Mitigate Visa Malfeasance Risks. GAO-06-115. October 6, 2005

Border Security: Strengthened Visa Process Would Benefit From Improvements in Staffing and Information Sharing. GAO-05-859. September 13, 2005

Border Security: Actions Needed to Strengthen Management of Department of Homeland Security's Visa Security Program. GAO-05-801. July 29, 2005.

Border Security: Streamlined Visas Mantis Program Has Lowered Burden on Foreign Science Students and Scholars, but Further Refinements Needed. GAO-05-198. February 18, 2005.

Border Security: State Department Rollout of Biometric Visas on Schedule, but Guidance Is Lagging. GAO-04-1001. September 9, 2004.

Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process. GAO-04-795. July 13, 2004.

Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars. GAO-04-371. February 25, 2004.

Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process. GAO-03-798. June 18, 2003.

Border Security: Implications of Eliminating the Visa Waiver Program. GAO-03-38. November 22, 2002.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. November 15, 2002.

Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool. GAO-03-132NI. October 21, 2002.

Ongoing Reviews

Review of International Aviation Passenger Prescreening. Requested by the Chairman and Ranking Member, Committee on the Judiciary, and the Ranking Member, Committee on Homeland Security, House of Representatives. Report expected in the fall of 1006.

Review of the Department of State's Measures to Ensure the Integrity of Travel Documents. Requested by the Chairman, Committee on the Judiciary, House of

Representatives; Chairman John N. Hostettler and member Darrell E. Issa, Subcommittee on Immigration, Border Security and Claims, Committee on the Judiciary, House of Representatives; and, Chairman Lamar S. Smith, Subcommittee on Courts, the Internet, and Intellectual Property, Committee on the Judiciary, House of Representatives. Report expected in the spring of 2007.

Review of the Department of State's Effort to Address Delays in Visa Issuance. Requested by the Chairman and Ranking Member of the Committee on Government Reform, House of Representatives. Report expected in the spring of 2007.

Review of Immigrant Visa Processing. Requested by the Ranking Member, Committee on Homeland Security, House of Representatives. Report expected in mid-2007.

(320455)

PASSENGER-CARGO SECURITY GROUP
An Airline Security Trade Association

Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology & Homeland Security:

Hearing on "Keeping Terrorists Off The Plane: Strategies For Pre-Screening International Passengers Before Takeoff"

Testimony Submitted by
Leon Laylagian, Executive Vice President
Passenger-Cargo Security Group
Washington, DC
www.pcsg.us

Thursday, September 7, 2006

Chairman Kyl and distinguished members of the Committee, I thank you for the opportunity to be here today and to provide testimony on this most important issue – aviation security.

My name is Leon Laylagian; I am the Executive Vice President of Passenger-Cargo Security Group. PCSG, a trade association working with legislators, regulators and aviation security professionals is dedicated to providing solutions in efforts to improve aviation security. PSCG has a professional partnership with over 22,000 airline pilots, an affiliation with nearly 400,000 airline passengers; and numerous industry leaders. I am also an airline pilot of 17 years with over 12,000 hours in a variety of aircraft, both domestically and international. I have flown for 3 passenger carriers and presently fly a Boeing 757/767 for a major all-cargo airline. My airline security work began in 1993, and I have served in many different capacities with unions and grass roots efforts improving airline security. I have served on various government working groups including the TSA's ASAC for cargo security in 2003. I am a graduate of Embry-Riddle Aeronautical University, also having served in the United States Navy.

Dating back to the 1920's, U.S. airlines have earned a large share of their revenue from freight and mail. Prior to September 11, 2001, many major passenger airlines carried more freight-ton miles than the major all-cargo airlines. After 9/11, security requirements decimated passenger airlines ability to earn this important revenue. While regulations were put in place to screen 100% of checked passenger bags, belly freight and mail had different rules.

With respect to freight, the TSA allowed the reintroduction of packages on passenger airlines that were "screened" by the Known Shipper program. Since the Known Shipper program simply shows the paper trail of the chain of custody for a given shipment, screening in this context is in stark contrast to inspection. The Known Shipper program did nothing to prevent Charles McKinley from shipping himself from New York to Texas; this demonstrates access. This was discussed and debated during the 2003 ASAC, however, the TSA decided to canonize the Known Shipper program as a method of screening. While an effort exists to enhance the Known Shipper program through continued working group process called the Freight Assessment System, now titled the Cargo Working Group, not much progress is being made. The TSA has not created a central data

base, and continues to allow shippers to manage their own lists. While this protects proprietary customer data, it does not enable what could be a very useful layer of security to serve as a package profiler. An enhanced Known Shipper program would be a very useful tool to decide what packages would undergo a further electronic inspection. Alone and without refinement, the Known Shipper program is a stop-gap measure.

Technology application for cargo inspection ideally should be 100%, however this is prohibitive with respect to throughput. A meaningful inspection formula would require 40% using electronic or physical means, with the 40% chosen by an enhanced Known Shipper program. The enhanced Known Shipper program would also go beyond a "yes or no" proposition, and delineate from "green, yellow, orange, and red" to better articulate the need for inspection. While there are presently 400,000 known shippers, hundreds of thousands more are involved in the supply chain. An additional random screening feature should be added to this inspection process.

Presently, a low percentage of cargo is inspected by either physical means, or available technologies. In the U.S., Explosion Detection Systems (EDS) are used to inspect passenger bags, and can handle broken bulk cargo. EDS produces an x-ray like image, and will alarm for the operator when an identified threat is recognized. Other available equipment includes Explosive Trace Detection (ETD, or spectral analysis) which takes a sample of particulate either by contact or forced air and tests the sample. This can be a desk top unit, or as large as an enclave. There is the TRX, or TIP (Threat Image Projection) Ready X-ray, otherwise known as the "enhanced screener" or the screening portal x-ray machine, which is not the most effective for detecting explosives. Another extremely effective tool is the K-9; while readily available and very accurate for explosive detection, K-9's do have a limited sensitivity and attention span. A technology that nearly matches the K-9 is Florescent Polymer. Florescent Polymer works very similar to the K-9, and like the dog, can detect liquid explosives. Other technologies include Gamma and Neutron based systems which have limited applications due to the problems they can cause for shipped contents, such as biomedical items.

Internationally, technology is used effectively to inspect cargo in several countries, and they have developed a proven track record of mitigating smuggling, contraband, and terrorist related shipments. These countries

include the United Kingdom, Amsterdam, Germany, France, Switzerland, Israel, Japan, China, Australia, and others. The first three utilize High Energy X-ray which cannot recognize the chemical structure of material, but still provides a lot of information with respect to operator interpretation. The United Kingdom and Amsterdam have High Energy X-ray equipment that is over 5 years old, and is considered to be performing successfully. In France, cargo is contained in a room, air is forced over the cargo to release particulate, and then the air is evacuated from the room through a filter. The filter is then examined by K-9's. In Israel, they begin with the nature of the shipment, since different types deserve different techniques. Switzerland (and others) uses Sub Pressure Simulation, or altitude chambers. Clearly, different tools are available for a variety of throughput, and risk assessment needs. Additionally, in China, they not only build their own equipment for cargo inspection, they inspect the supply chain, and require the build-up of freight to take place at the airport of departure.

At the screening portals, the ability to keep threat material, such as explosives, off the aircraft cannot depend on the TIP Ready x-ray machines and individual TSA screeners alone. The TSA is to be commended for implementing Behavior Pattern Recognition (BPR) which they now call the SPOT program. While this is a good beginning, it is far from being sufficient. The SPOT program only teaches TSO's how to detect suspicious behavior, and not how to ask the important questions that actually make BPR work. That role is delegated to the airport law enforcement officers, who are the backbone of the airport security. These law enforcement officers, however, are not trained in BPR. Given the explosive threat, the Richard Reid "shoe bomber" incident provides a good example. Mr. Reid was selected by security screeners, and was questioned by the French airport police. Their training was focused on criminal activity, not terrorist behavior, and therefore they released him to travel on a subsequent flight. In the U.S., Boston Logan airport hired BPR originator, Mr. Rafi Ron, to train the Massport police. To date, the police at the Boston airport report that non-terrorist related arrests have significantly increased due to the application of the BPR program. The Boston police move throughout the entire airport environment. The SPOT program resides solely at the screening portal, and does not use the effective BPR tools anywhere else in the airport environment. A properly run BPR program in combination with K-9's can be very effective at mitigating many types of "carry on explosives" Given the restrictions that international operations may pose, it would be extremely effective to train U.S. pilots that

fly to international destinations in the BPR program. These crewmembers stay in the hotels, travel through the communities, enter the airport(s) from the curb, and transit all the way through the sterile side of airport operations. As the most vetted aviation employees in the system, and given their mobility, they are uniquely qualified to perform a BPR function at foreign airports. Various airport and airline employees stove pipe their training, and are not well integrated with respect to application and response with other employee groups.

Technology is an important tool for cargo inspection, and the lack of direction and will, prevent its refinement and use. Do we "buy the computer today, or do we wait two months for improvements"? We cannot wait for magic solutions, and while many technologies are not perfect at this time, they are significantly more effective than doing nothing. We also cannot ignore the human element and the value of ongoing intelligence, and placing that intelligence in the right hands. With very few exceptions, crewmembers still do not have access to Security Directives or Information Circulars.

In closing, we urge Congress to work together to ensure that the security of both cargo and passengers airlines – and the flying public - are not compromised by overlooking yet another aviation security loophole.

Thank you again Chairman Kyl and distinguished members of the Committee for the opportunity to provide testimony. I welcome any questions.

TESTIMONY OF PAUL S. ROSENZWEIG
COUNSELOR TO THE ASSISTANT SECRETARY FOR POLICY
AND
JAYSON P. AHERN
ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
BEFORE
THE SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

Chairman Kyl, Ranking Member Feinstein, and other distinguished Members of the Subcommittee, we are pleased to join you this afternoon to discuss the ongoing efforts of the Department of Homeland Security (DHS) to prevent terrorists from both entering the United States and posing a threat to international air travel.

DHS was born in the aftermath of the most horrific terrorist attack on the United States and the aviation system in history. "Keeping terrorists off the plane," both at home and abroad, has been a central priority for the Department. This is why both air travel and how we vet arriving travelers have changed fundamentally.

The recently dismantled plot to blow up aircraft en route to the United States from Britain reinforces the severity and the importance of our challenge. It reminds us not only that terrorists remain intent on targeting air travel, but of the importance of a layered approach to security, an approach that is supported by close interagency and international cooperation. It's instructive to recall that what could have been the second largest terrorist attack on aviation was disrupted far from the airport. Nonetheless, it was aviation security officials in the United States and London who cooperatively responded to the new environment that investigators presented to them.

Integration of efforts and cooperation with allies are at the forefront of DHS's strategy to identify and interdict those who would do us harm before they can board an aircraft for the United States. Our efforts begin well before the airport, and include both the visa issuance process and decisions to exempt travelers from certain countries from that process. Our efforts continue in the days and weeks leading up to the departure of an aircraft as we receive critical data about the flight, assess it, and, in some cases, alert U.S. Customs and Border Protection (CBP) officers stationed oversees to work with their counterparts to further vet and interdict high risk travelers. This entire process is further supported by the work of Customs and Border Protection and the Transportation Security Administration (TSA) – in partnership with foreign governments, air carriers, and airports – to ensure that passengers and their baggage are properly screened before boarding an aircraft departing for the United States.

We'd like to take a few moments to update you on some of the most critical programs that support our layered-security approach, including the Visa Waiver Program (VWP), our use of Advance Passenger Information and Passenger Name Records to prescreen travelers, and overseas activities to support point of departure screening.

First, DHS is committed to further strengthening the Visa Waiver Program's security features. With almost 16 million people entering the U.S. under this program each year – a number that represents more than one-half of all non-immigrant admissions (excluding those from Canada and Mexico) – the VWP is at the forefront of our efforts to facilitate international travel. It is also at the forefront of our efforts to defend against those from VWP countries who seek to abuse America's welcoming nature.

Originally established in 1986, the VWP allows citizens of designated countries – of which there are currently 27 – to travel to the United States for business or pleasure for up to 90 days without a visa. By permitting qualified low-risk countries to join or remain part of this program, the United States has promoted better relations with allies, eliminated unnecessary barriers to travel, stimulated the tourist industry, allowed U.S. consular offices to focus on higher priority visa screening, and encouraged international cooperation against organized crime, trafficking in persons, drug smuggling, and terrorism.

DHS has used the Visa Waiver Program's existing procedures to set strict security standards for member countries, as well as to enforce milestones for their completion. This is done through frequent assessments on the ability of the 27 VWP countries to meet a host of security guidelines that are constantly being strengthened. Because a passport is the sole document a citizen from a VWP country must have to enter the United States, we must ensure that passports issued by VWP countries meet the most exacting security standards. Accordingly, all VWP country passports issued after October 25th of this year must be "e-passports," which contain a chip to store the user's biometric and biographic information. This change incrementally builds off of an already strict standard instituted last October that requires VWP passports issued after that date to include a digital photo, be machine-readable, and be tamper-resistant. In addition, all VWP travelers were enrolled into the US-VISIT program – which collects fingerprints and photographs from visitors to the United States – as of September, 2004. Combined, these features will make it very difficult for anyone other than the official holder of the passport to enter this country.

As the Subcommittee knows, the Government Accountability Office recently issued several reports on DHS's administration of the VWP. DHS appreciates GAO's continued support for this vital program and its recommendations for improving it. In fact, DHS already has addressed many of the issues GAO identified. For instance, GAO recommends a clear standard operating procedure for the reporting of lost and stolen passport data from foreign governments to the U.S. The Office of International Enforcement already has developed and cleared standards to implement such a policy. Those standards include timely reporting, procedures for reporting, and improved distribution for U.S. officials who need access to such information. Further, DHS is working closely with Interpol to ensure that, as part of the pre-departure screening process, all travelers' passport information vetted against Interpol's lost and stolen travel document database, which contains nearly 12 million records.

Since 2004, the Office of International Enforcement improved the country review process – a review that each VWP country must undergo every two years to determine its continued participation in the program. For instance, we have developed new standard operating procedures for the review, implemented a training program for the country review teams, and

streamlined the review process to target the issues of greatest concern to the U.S. We may also develop a continuous review process that would be more targeted and effective than the "rear view mirror" approach that we currently take every two years.

While the Visa Waiver Program is an important tool in the war on terrorism, there is room for improvement. The existing VWP assesses risks to the United States on a country-by-country basis; the law assumes that a citizen who hails from, say, Britain, poses no threat to the American people. That sort of assumption is no longer sound. The Visa Waiver Program also needs to look for risks on a traveler-by-traveler basis. The Department looks forward to working with Congress to further enhance the VWP's security features as new countries are considered for admission into the program.

Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate *bona fide* travelers so it can focus its resources on areas of highest risk.

The Advance Passenger Information System (APIS) was developed in 1988 in cooperation with the airline industry. At that time, air and sea carriers voluntarily collected passenger and crew biographical data – typically information that would be on the aircraft manifest or the individual's passport – and transmitted this data to the United States Government while the vessel or aircraft was en route to this country.

Current CBP regulations require that an air carrier must electronically transmit passenger arrival manifests to CBP no later than 15 minutes after the departure of the aircraft from a foreign port; carriers also have to electronically transmit passenger departure manifests no later than 15 minutes prior to departure of the aircraft from the U.S. port of departure. Manifests for crew members (on passenger and all-cargo flights) and non-crew members (limited to all-cargo flights) must be electronically transmitted to CBP 60 minutes prior to the departure of any covered flight from a foreign port and 60 minutes prior to the departure of any covered flight from the U.S. port of departure. (A "covered flight" is one to, from, continuing within, or overflying the United States.) Sea carriers are similarly regulated, but with different timeframes for the transmission of the manifest data.

Shortly after the September 11 atrocities, DHS recognized the need to have APIS information provided in advance of an aircraft's departure. Without knowing exactly who is on board an aircraft prior to its departure, our ability to prevent hijackings or suicide attacks is greatly inhibited. Congress saw the need, as well and codified this principle in section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004. As a result, after extensive consultations with our international partners, DHS on July 14, 2006 published the pre-departure Notice of Proposed Rule Making. After evaluating several alternative approaches, the proposed rule offers two options for carriers to transmit passenger data to DHS, in a manner sufficient to allow DHS to screen all passengers prior to the departure. Specifically, air carriers could transmit complete manifests no later than 60 minutes prior to departure. Or they could transmit passenger data as individual, real-time transactions as each traveler checks in, up to but no later than 15 minutes prior to departure. The proposed rule also recommends changing the definition of "departure," as set forth in 19 C.F.R. § 122.49a, to mean "from the moment at which the aircraft is pushed back from the gate."

If the rule is finalized and implemented as proposed – the comment period will close on October 12 of this year – the United States Government would take on the watch list screening responsibility for all travelers arriving into or departing from the United States aboard a commercial aircraft or vessel. This would eliminate the current responsibility of carriers flying into the United States to check the No Fly and selectee lists. It also would bring greater control over this process into government hands.

The information available from Passenger Name Records (PNR) is distinct from, but every bit as important as, Advance Passenger Information. PNR is information contained in an air carrier's electronic reservation system and/or departure control system that describes the identity and travel plans of a passenger or group of passengers included under the same reservation. This data is more extensive than what DHS receives through APIS and conceivably could contain upwards of 50 fields – including information such as travel history, seat assignments, contact phone numbers, and form of payment. The greater depth and breadth of this information makes it a vital tool for a thorough vetting of all passengers. While API allows us to complete checks against watchlists and other records with great accuracy, it does not always include information that would allow us to link an unknown adversary or "clean skin" to known or suspected terrorists and criminals.

CBP has been using PNR data since 1992, when it was a voluntary program begun in cooperation with fourteen airlines. On November 19, 2001, President Bush signed into law the Aviation and Transportation Security Act, which mandated that carriers make PNR data available to CBP. As a result, CBP published an interim rule in 2002 that requires all air carriers operating passenger flights in foreign air transportation to and from the United States to provide CBP with electronic access to PNR data to the extent that it is collected and contained in their reservation and departure control systems. CBP is currently collecting PNR data from 127 airlines, which represents all major carriers operating to and from the United States.

DHS's use of PNR and APIS information has produced a number of successes in the war on terrorism. Using these data, CBP has encountered 4801 positive matches for known or suspected terrorists.

Despite PNR's success stories and 15 year history, the European Union in 2003 approached DHS and expressed concerns about the status of the program under European privacy laws. The result, in 2004, was an agreement that legally protected carriers that complied with the CBP regulation. But the agreement has also limited the ability of counterterrorism officials to have broad access to PNR data and to hold the data long enough to support future investigations. As the Subcommittee knows, in May the European Court of Justice (ECJ) annulled this agreement due to a technicality in European law. The European Union has since notified the United States that the agreement will be terminated at the end of this month.

We are actively engaging the European Union to develop an appropriate replacement agreement. However, it is important to emphasize DHS's belief that the ECJ's ruling should not impact international air travel. The court did not rule that DHS's access to and use of PNR violated European privacy law. Nor did the court seek to curb carrier compliance. In fact, it ruled that the European-wide privacy directive does not apply to DHS's collection and use of PNR. Likewise, after extensive review, the DHS Chief Privacy Officer in September 2005 determined that CBP's use of PNR was in compliance with the representations made in the Undertaking and followed the standards of fair information practices. As such, DHS expects all carriers serving the U.S. market to continue complying with current regulations.

It is also important to keep the overall stakes in mind. The primary lesson from 9/11 was that we cannot effectively combat the terrorist threat if we prevent our law enforcement and counter terrorism agencies from communicating and cooperating. In 2004 Congress passed the Intelligence Reform and Terrorism Prevention Act to ensure that those mistakes are never repeated. Prior to 2004, however, our Immigration and Customs Enforcement investigators effectively used PNR information to combat a host of crimes. Today they are unnecessarily hindered in their ability to use European data to do so. That said, DHS is strongly encouraged by recent statements by European Commission Vice President Franco Frattini and looks forward to developing a mutually acceptable, long term, cooperative arrangement with our European allies.

All of these efforts to separate high and low risk travelers are necessarily supported by DHS programs overseas and by cooperation with our friends and allies. Both CBP and the Transportation Security Administration maintain programs in foreign countries that greatly enhance our prescreening efforts. For instance, the Immigration Advisory Program (IAP) works with airline carriers and host country authorities to identify potentially inadmissible travelers who may pose a threat to the national security. With this added security layer, CBP can reduce suspected overseas threats prior to the flight's departure, thereby avoiding delaying, canceling, or diverting flights destined for the United States.

The IAP teams have no legal authority in these foreign countries, but have forged strong relationships with local law enforcement. Through cooperation they are able to further vet high risk passengers based on information held by the host government and coordinate a response. They may also recommend to the air carrier that the passenger suspected to be traveling on

fraudulent documents not be allowed to board the flight. Although an air carrier is not required to abide by the recommendation, it may be liable for fines and for the cost of returning the passenger to the country of departure if CBP subsequently denies him or her entry to the United States.

IAP was initiated at two locations in FY 2004: at Amsterdam – Schiphol International Airport in June, and Warsaw – Chopin International Airport in September. IAP expanded to the London – Heathrow International Airport as a 120-day pilot in April 2006, and subsequently extended an additional 120-days ending December 2006. The establishment of a fourth site at Tokyo – Narita International Airport has just been agreed to by the Japanese government. Pending host government approval, CBP's fiscal year 2007 budget includes converting Amsterdam, London, and Tokyo to permanent locations.

As of August 24, 2006, IAP teams have made more than 700 no-board recommendations for high-risk or inadequately documented passengers. They also have intercepted 78 fraudulent documents. These accomplishments equate to approximately $1.6 million in avoided costs associated with detaining and removing passengers who would have been returned after having been refused admission to the United States, and $1.5 million in air carrier potential savings for fines and passenger return costs.

Similarly, DHS works with individual carriers and airports to ensure their processes for physically screening each passenger prior to boarding meet adequate standards. Our goal is to ensure that carriers and airport authorities remain a critical partner in identifying those that may be trying to travel on fraudulent documents or threaten the aircraft.

Despite all our prescreening programs, it is still important to have trained eyes reviewing a person's documentation to confirm they are who they claim to be. Other than the airports at which IAP is active, the first opportunity DHS has to make such a determination for an international passenger is after the passenger disembarks from the aircraft. The Carrier Liaison Program (CLP) was developed to enhance border security by helping commercial carriers identify improperly documented passengers who are traveling to the United States. The CLP provides training and technical assistance directly to carrier staff on topics such as U.S. entry requirements, passenger assessment, fraudulent document detection, and imposter identification. The program uses state of the art document examination material, equipment, and training tools. To date, CLP has trained over 1800 carrier personnel and security personnel.

Likewise, our electronic prescreening systems will never be able to identify all potential threatening passengers with a 100 percent degree of reliability. A single radical person can seek to carry out his own personal attack on an aircraft. As a result, it's equally critical that airline and airport personnel are properly trained and equipped to detect explosives and other weapons on a passenger or in their luggage. To this end, TSA regulates the security operations of all air carriers operating flights to the United States. Over 140 non-U.S. passenger air carriers and 30 non-U.S. all-cargo carriers have TSA-approved security programs for operations to and from the U.S. TSA is able to rapidly update these plans by issuing Emergency Amendments (EAs). The EA process proved critical in ensuring that all carriers received immediate notice of the recent ban on liquids and effectively implemented it.

To ensure these rules are being followed, TSA operates the Foreign Airport Assessment and Air Carrier Inspection Programs. During airport assessments conducted in foreign countries, International Aviation Security Inspectors focus on application of International Standards and Recommended Practices defined by the International Civil Aviation Organization, to which 189 countries are signatories. TSA international inspectors visit every airport that serves as a last point of departure for the United States, those locations where U.S. aircraft operators fly, and any site deemed necessary by the Secretary of Homeland Security. Each foreign airport assessment, mandated by law, is performed at least triennially. Nearly 270 airports are regularly visited by TSA inspectors and an average of 30 new inspection locations are identified each year, requiring comprehensive surveys and follow-on assessments. The air carrier inspection protocols focus on U.S. aircraft operators and foreign air carriers' compliance with applicable TSA regulations. Over 800 air carrier stations are inspected each year.

* * *

We've outlined many distinct DHS programs for you today. Each fills an important niche in securing the diverse activities that together comprise every international flight to the United States. The visa application process remains our first opportunity to vet a prospective traveler against our knowledge of known and suspected terrorists. As such, how we decide which friends and allies will be exempted from a visa requirement is a vital factor in adverting risk. Only through strong requirements regularly enforced can we prevent our close economic and cultural relationships from becoming a security liability. That said, the availability of extensive and reliable data long before departure remains our greatest asset. By applying the full force of the information and analytical capabilities of the U.S. intelligence and law enforcement communities, we can identify many threats and prevent them from evolving into disasters.

○