AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–103

# INTERRUPTING TERRORIST TRAVEL: STRENGTHENING THE SECURITY OF INTERNATIONAL TRAVEL DOCUMENTS

## HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 2, 2007

**Serial No. J–110–32**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
36–943 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

PATRICK J. LEAHY, Vermont, *Chairman*

| | |
|---|---|
| EDWARD M. KENNEDY, Massachusetts | ARLEN SPECTER, Pennsylvania |
| JOSEPH R. BIDEN, JR., Delaware | ORRIN G. HATCH, Utah |
| HERB KOHL, Wisconsin | CHARLES E. GRASSLEY, Iowa |
| DIANNE FEINSTEIN, California | JON KYL, Arizona |
| RUSSELL D. FEINGOLD, Wisconsin | JEFF SESSIONS, Alabama |
| CHARLES E. SCHUMER, New York | LINDSEY O. GRAHAM, South Carolina |
| RICHARD J. DURBIN, Illinois | JOHN CORNYN, Texas |
| BENJAMIN L. CARDIN, Maryland | SAM BROWNBACK, Kansas |
| SHELDON WHITEHOUSE, Rhode Island | TOM COBURN, Oklahoma |

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

---

## SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

DIANNE FEINSTEIN, California, *Chairman*

| | |
|---|---|
| EDWARD M. KENNEDY, Massachusetts | JON KYL, Arizona |
| JOSEPH R. BIDEN, JR., Delaware | ORRIN G. HATCH, Utah |
| HERBERT KOHL, Wisconsin | JEFF SESSIONS, Alabama |
| CHARLES E. SCHUMER, New York | JOHN CORNYN, Texas |
| RICHARD J. DURBIN, Illinois | SAM BROWNBACK, Kansas |
| BENJAMIN L. CARDIN, Maryland | TOM COBURN, Oklahoma |

JENNIFER DUCK, *Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS


| | Page |
|---|---|
| Feinstein, Hon. Dianne, a U.S. Senator from the State of California | 1 |
| Schumer, Hon. Charles E., a U.S. Senator from the State of New York | 17 |
| Kyl, Hon. Jon, a U.S. Senator from the State of Arizona | 4 |


## WITNESSES


| | |
|---|---|
| Donovan, Patrick D., Assistant Director for Diplomatic Security, Director of Domestic Operations, Bureau of Diplomatic Security, Department of State, Washington, D.C. | 7 |
| Ervin, Clark Kent, Director of Homeland Security, Aspen Institute, and Former Inspector General, Department of Homeland Security, and Author, Washington, D.C. | 26 |
| Everitt, Michael P., Unit Chief, Forensic Document Laboratory, Immigration and Customs Enforcement, Department of Homeland Security, Washington, D.C. | 9 |
| Morris, Paul, Executive Director, Admissibility Requirements and Migration Control, Office of Field operations, Customs and Border Protection, Department of Homeland Security, Washington, D.C. | 12 |
| Noble, Hon. Ronald K., Secretary General, Interpol, Lyon, France | 23 |
| Simkin, Andrew, Director, Office of Fraud Prevention Programs, Bureau of Consular Affairs, Department of State, Washington, D.C. | 5 |
| Zimmer, Brian, Senior Associate, Kelly, Anderson & Associates, and Former Senior Investigator, Committee on the Judiciary, U.S. House of Representatives, Washington, D.C. | 28 |


## QUESTIONS AND ANSWERS


| | |
|---|---|
| Responses of Andrew Simkin to questions submitted by Senators Feinstein and Schumer | 37 |
| Responses of Paul Morris and Michael Everitt to questions submitted by Senators Schumer and Feinstein | 45 |


## SUBMISSIONS FOR THE RECORD


| | |
|---|---|
| Donovan, Patrick D., Assistant Director for Diplomatic Security, Director of Domestic Operations, Bureau of Diplomatic Security, Department of State, Washington, D.C., statement | 61 |
| Ervin, Clark Kent, Director of Homeland Security, Aspen Institute, and Former Inspector General, Department of Homeland Security, and Author, Washington, D.C., statement | 66 |
| Everitt, Michael P., Unit Chief, Forensic Document Laboratory, Immigration and Customs Enforcement, Department of Homeland Security, Washington, D.C., statement | 72 |
| Kephart, Janice, former Counsel, 9/11 Commission and President, 9/11 Security Solutions, LLC | 84 |
| Morris, Paul, Executive Director, Admissibility Requirements and Migration Control, Office of Field operations, Customs and Border Protection, Department of Homeland Security, Washington, D.C., statements | 87 |
| Noble, Hon. Ronald K., Secretary General, Interpol, Lyon, France, statements | 94 |
| Simkin, Andrew, Director, Office of Fraud Prevention Programs, Bureau of Consular Affairs, Department of State, Washington, D.C., statement | 115 |

Page

United States Department of State, Washington, D.C., Visa and Passport Security Strategic Plan ..... 127

Zimmer, Brian, Senior Associate, Kelly, Anderson & Associates, and former Senior Investigator, Committee on the Judiciary, U.S. House of Representatives, Washington, D.C., statement and attachments ..... 167

# INTERRUPTING TERRORIST TRAVEL: STRENGTHENING THE SECURITY OF INTERNATIONAL TRAVEL DOCUMENTS

---

**WEDNESDAY, MAY 2, 2007**

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

The Subcommittee met, pursuant to notice, at 10:00 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, Chairman of the Subcommittee, presiding.

Present: Senators Feinstein, Schumer, and Kyl.

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

Chairman FEINSTEIN. I would like to call this Subcommittee meeting to order. My Ranking Member, Senator Kyl, is here. I believe we will be joined by Senator Schumer, who has asked to make a statement, and, of course, we will afford him that opportunity.

We are going to try to move this as quickly as possible. Senator Kyl has a critical appointment at around 10:30, and I have one at noon. But this is an important Subcommittee, and I would just like our witnesses to try to think about what they are going to say and say it in as close to 5 minutes as you possibly can. And I will begin with a statement that hopefully will set the parameters for the hearing.

For terrorists, international travel documents are as important as weapons. Now, that is not my statement. That is the conclusion of the authors of the 9/11 report over 5 years ago. The 9/11 report pointed out that international travel presents greater danger to terrorists because they must surface to pass through regulated channels. They must present themselves to border security officials or attempt to circumvent inspection points.

The moment that the terrorist presents a false document to Border Patrol inspectors is a critical moment in the protection of our borders. In that short, brief interview at the border point, the officer must be able to determine whether the person attempting to enter the United States intends to harm the people of this country.

Today there are many tools that a border inspector or the consular officer or other Government agents can use to identify real travelers from those with bad motives. The ongoing question and

the reason we are here today is whether United States Government agencies are taking advantage of all those tools.

This is a subject we come back to over and over again in this Subcommittee, and this is a subject that is extremely important to me. I am not going to rest until I believe that the United States Government is taking all the security measures it can take to interrupt terrorist travel.

The point of this hearing today is to assess where we are and where the Government still needs to improve when it comes to document security. We cannot be complacent when it comes to this subject. The evidence has shown repeatedly that false travel documents provide a gateway for organized crime and terror.

The 9/11 terrorists devoted extensive resources to acquiring and manipulating passports, all to avoid detection of their nefarious activities and objectives. We know, for example, that at least two of the 9/11 hijackers used passports that were altered when they entered this country, and as many as 15 of the 19 had some other irregularity with their travel document.

In the 5 years since 9/11, of the 353 individuals who the Department of Justice classified and prosecuted as international terrorists, 24 were charged with document crimes. For example, in September of 2005, Mohammed Khalil was convicted on several visa fraud charges. Mr. Khalil was the ringleader of a massive visa fraud scheme operating out of a mosque he established in a Brookyln basement. Over a 10-year period, Khalil sponsored over 200 fraudulent applications for individuals seeking religious work visas to enter the United States, charging cash fees ranging from $5,000 to $8,000 dollars. Prosecutors claim that he netted more than $600,000 from the scheme.

Although Khalil has not been linked to specific terrorist activities, prosecutors pointed to a taped conversation in which Khalil reportedly praised Osama bin Laden and called for Muslims to arm themselves for another attack.

In another case, defendants Cedric Carpenter and Lamont Ranson were prosecuted and sentenced in Mississippi for conspiring to sell false documents to individuals they believed were members of Abu Sayyaf, a Philippine-based group designated as a foreign terrorist organization.

In my own home State of California, seven counterfeit document mills in Los Angeles were seized on March 30, 2006. ICE agents arrested 11 individuals on charges of supplying a significant number of the fraudulent identity and immigration documents being sold on the streets of Los Angeles.

Now, it is true most of this is to bring people illegally across the border, but, nonetheless, there is no safeguard on how these false documents can be used.

And just this past December, the United States Department of State's Diplomatic Security Service charged 25 defendants in Los Angeles for attempting to obtain and actually obtaining United States passports using fake identities.

Today, over 5 years later, Interpol reports that they have records of more than 12 million stolen and lost travel documents from 113 different countries. Now, these are the only ones we know about, but Interpol is a vast source of information. And as far as I know—

and I am sure these witnesses will correct me if I am wrong—the Government does not scan passports to pick up on the Interpol data, which I think is a significant lapse if, in fact, it is true. Interpol estimates that 30 to 40 million travel documents have been stolen worldwide.

We know that over the past few years, passport and visa forgery has become more sophisticated thanks to new technology. In the past, the tools of the counterfeit document trade were typewriters and pieces of plastic. Today's document forgers use computer software and high-resolution digital scanners to ply their trade. Criminal organizations are also using the Internet to market and distribute fake documents and immigration benefits to customers.

It is not only foreign passports that can be forged. Forged and fraudulent United States passports can be most dangerous when in the wrong hands, because with a U.S. passport criminals can establish American citizenship and have unlimited access to virtually every country in the world.

Despite evidence that these crimes are widespread and that millions of travel documents are on the black market, in 2004 the State Department's Diplomatic Security Service reports that it made about 500 arrests for passport fraud with only 300 convictions.

For these reasons, I believe that our job is not over. Senator Sessions and I have introduced a bill to strengthen current passport and visa laws in a number of key ways. Our bill would create strong penalties to punish those who traffic in fraudulent travel documents. This must happen. The current law makes no distinction between those caught with multiple false travel documents, the very worst offenders who are often part of organized crime rings, and those with only one false document. Our bill would change that.

We would also add provisions to the current passport and visa fraud laws to ensure that conspiracies and attempts to commit these crimes are investigated and prosecuted just as vigorously as the completed crime. Currently, offenders who engage in passport or visa fraud generally serve less than a year in prison, providing little incentive for U.S.

Attorney's Offices to expend scarce resources in prosecuting these crimes, and that is a big problem.

So we think our bill provides much needed reform. It strengthens the penalties against people using documents to illegally gain entry to this country and empowers the agents and prosecutors who enforce our borders to take swift and strong action against these criminals.

So I hope my colleagues, including my colleague on the right, will join Senator Sessions and me in cosponsoring this important legislation. But legislation is not enough. The Department of Homeland Security and State Department must work with Interpol to ensure that the front-line inspectors, those at airports and consular offices, have real-time access—real-time access—to lost and stolen passport databases. The inspectors must be trained to use these databases to ensure that no one carrying a stolen passport is allowed into this country.

So that is what this hearing is all about. We have very credible and informed witnesses, and I would like to turn it over to my Ranking Member, with whom I have worked now on this Committee I guess for at least 10 years.

Senator KYL. Over 12 years now.

Chairman FEINSTEIN. Over 12 years.

Senator KYL. Time flies when you are having fun.

Chairman FEINSTEIN. It has been a great pleasure for me. Senator Kyl.

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

Senator KYL. Madam Chairman, thank you, and let me begin by thanking you for holding this hearing.

First let me say that I agree with everything you have said. This is a bipartisan issue. We have worked in this Subcommittee in a very constructive and bipartisan way now for over 12 years, and it is a pleasure always to work with you, now to be your wing man now that the political tables are slightly turned here. It does not make any difference in this Subcommittee.

But this is an excellent complement, actually, to a hearing that we held last September when we focused on ways of how to improve the security of international flights to the United States without necessarily interfering—or disrupting, I should say, the travel for many millions of people who fly here every day.

But Senator Feinstein is absolutely right that complacency could be one of our main enemies here. We should recall that 9/11 began, with all due respect, to the State Department's inadequate interviews—actually, they had contracted it out to private parties—and inadequate review and document inspection, which allowed the 9/11 hijackers to come in and stay in the United States.

It seems to me the question now is not so much how much progress we have made, but how much more we need to do. If another 9/11 were to happen, people would ask would more could have been done, and I think everybody here today—and judging from some of the statements that I have read of the witnesses, it is clear that everyone agrees that more reasonably can be done.

I would like to thank all of the witnesses for being here today and especially a couple that I have contacted, Secretary General Ron Noble of Interpol, for joining us. Our office has been in contact and working to improve security, and Senator Feinstein has discussed that. And also Mr. Brian Zimmer. The appendix in Mr. Zimmer's testimony on the Federal laws that Congress has passed to improve Federal identity documents is a very good summary, and I think that will be very helpful to us.

The arrival of international terrorism to our shores has made us all aware of the need for improved security at our borders and ports of entry. We have had to adapt to a much more sophisticated enemy than I think any of us had thought when the terrorist attacks first occurred. And we have had to adapt with more sophisticated screening mechanisms, identity documents, data sharing, and the like.

So the testimony that I think we will hear today, again, while it shows that we have come a long way, I think will also reveal how

much more work remains to be done. And our obligation here in Congress will be to continue to initiate efforts such as Senator Feinstein mentioned, as well as to work with the administration to improve domestic security, pass meaningful legislation that addresses the gaps in security, and importantly then to provide the funding that is necessary to effectuate the changes that we all believe are necessary. So again, Senator Feinstein, thank you for holding this very important hearing.

And as Senator Feinstein said, I will have to leave just before 10:30, and please know that that in no way detracts from my interest in this. And I may have questions that I will want to submit to the witnesses as a result of the oral testimony here.

Thank you, Madam Chairman.

Chairman FEINSTEIN. Thank you very much, Senator.

I might say that Ron Noble is the Secretary General of Interpol, and he has come here from Lyon, France, and we very much appreciate it. He will lead off on the second panel. But I would like to introduce the first panel to you, and we will go right down the line.

The first person testifying will be Andrew Simkin. He is the Director of Fraud Prevention Programs, the Bureau of Consular Affairs of the Department of State.

The second person will be Patrick Donovan, the Assistant Director for Domestic Operations and Acting Director of Diplomatic Security for Counter Measures of the Department of State.

And Michael Everitt, the Unit Chief of the Forensic Documents Laboratory, Immigration and Customs Enforcement, the Department of Homeland Security.

And then, finally, Paul Morris, the Executive Director of Admissibility Requirements and Migration Control, Office of Field Operations from United States Customs and Border Protection.

So as you can see, this is a very qualified and credible panel, and I just hate to do it, but we would like to ask questions. So if you could say what you mean in 5 minutes, it would really be appreciated, and I will ask the clocks to be started. Thank you very much.

Mr. Simkin, may we start off with you.

## STATEMENT OF ANDREW SIMKIN, DIRECTOR, OFFICE OF FRAUD PREVENTION PROGRAMS, BUREAU OF CONSULAR AFFAIRS, DEPARTMENT OF STATE, WASHINGTON, D.C.

Mr. SIMKIN. Thank you, Chairman Feinstein, Ranking Member Kyl. I appreciate this opportunity to discuss the work that we do to interrupt terrorist travel. It is a tremendously important topic for America, and it is one to which I have dedicated a lot of thought and effort over my 20 years of service as a consular officer.

As you indicated, Chairman Feinstein, the staff members of the 9/11 Commission identified travel as some of the key moments for interrupting terrorists' activities. One comparison that I heard was comparing terrorists to submarines operating in hiding most of the time, but needing to surface at key moments, making them more vulnerable to detection. When a terrorist applies for a visa to enter our country, it is a key moment of opportunity for us to interrupt his travel. Airline check-in and port-of-entry screening are other key moments.

I would like to describe some of the things that we are doing to take maximum advantage of those opportunities.

Our systems for checking names and biographic data against terrorist watchlists and other databases are more comprehensive and sophisticated than ever before. Thanks to interagency data sharing, we are making good progress in international sharing of data on known terrorists and data on lost and stolen passports. We have added biometric capabilities using both fingerprinting and facial recognition technology to identify persons who may be applying for visas under false identities. We recently began the rollout of an upgrade from a two-fingerprint system to ten prints. This transition should be finished by December of this year.

Bearing in mind that many persons with criminal intent have no known record and, thus, do not appear in any biographic or biometric database, we take advantage of personal interviews conducted by consular officers specially trained to observe demeanor and detect inconsistencies, who ask applicants all sorts of questions. In addition to the interview, consular officers use an increasingly sophisticated array of techniques and technologies to defeat visa fraud.

By law, the burden of proof is on the applicant. On an average day at over 200 posts around the world, we turn away 5,000 foreign nationals who do not qualify for visas because they fail to meet that burden of proof.

The terrorist's travel may be deterred by the risk that he might not only be refused a visa, but that information we gather from his application, including fingerprints, phone numbers, et cetera, may compromise his entire operation. We work closely with DS, DHS, and other U.S. Government colleagues to follow up on cases of suspected fraud or security concerns.

Along with our efforts to prevent terrorists from receiving U.S. travel documents, we also seek to safeguard the integrity of visas and passports against alteration, forgery and misuse. We share our U.S. visa and passport databases with our Customs and Border Protection colleagues so that any document can be electronically verified.

The U.S. passport was also recently completely redesigned, incorporating multiple new security features, including an electronic chip, and I have brought samples of the new passports for the Committee.

Chairman FEINSTEIN. These are fraudulent passports?

Mr. SIMKIN. No. These are genuine. I believe you each should have one sample of the e-passport, which is the regular passport, with the symbol on the cover indicating electronic chip. And the other sample is the emergency photo digitized passport.

Chairman FEINSTEIN. This is the symbol?

Mr. SIMKIN. Correct, yes. The other is the new emergency photo digitized passport, which is now in effect at all of our posts overseas, issued to persons who have emergency travel, such as having lost a passport overseas. These are issued for up to one year of validity.

Chairman FEINSTEIN. Could you provide the Committee with some samples of fraudulent passports so we might—

Mr. SIMKIN. We certainly could.

Chairman FEINSTEIN.—see the different technique used.

Mr. SIMKIN. We would be happy to.

Chairman FEINSTEIN. Please continue.

Mr. SIMKIN. OK. In conclusion, I thank you for your interest in the work of consular officers, who truly work the front line in interrupting terrorist travel while at the same time serving as the public face of America, showing fairness and consideration in dealing with millions of legitimate travelers.

I look forward to answering your questions.

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

Chairman FEINSTEIN. Thank you very much, Mr. Simkin.

Mr. Donovan?

**STATEMENT OF PATRICK D. DONOVAN, ASSISTANT DIRECTOR FOR DOMESTIC OPERATIONS OF THE DIPLOMATIC SECURITY SERVICE, BUREAU OF DIPLOMATIC SECURITY, DEPARTMENT OF STATE, WASHINGTON, D.C.**

Mr. DONOVAN. Good morning, Madam Chair and Ranking Member Kyl. I am honored to appear before you today with my distinguished colleagues. I would like to thank you and the Committee members for your continued support and interest in the Bureau of Diplomatic Security's protective and investigative programs. I would especially like to thank you for your support in strengthening passport and visa legislation. Through congressional support, DS safeguards American diplomats and facilities around the world and protects the integrity of U.S. travel documents. With your permission, I would like to present a brief statement and submit a copy of our Visa and Passport Security Strategic Plan as my full testimony for the record.

One of the most critical national security challenges that the American people will face for the foreseeable future is the desire by terrorist groups and individuals to inflict catastrophic harm upon the United States. A key element in all terrorist operational planning is access to the target. Such access requires the acquisition of travel documents, including visas and passports—

Chairman FEINSTEIN. Could you pull the mike down just a little bit, please?

Mr. DONOVAN. I am sorry, ma'am?

Chairman FEINSTEIN. Pull the mike a little bit down. I think you will pick up better. Thank you.

Mr. DONOVAN. Such access requires the acquisition of travel documents, including visas and passports, that allow terrorists to enter, and move freely within, our country.

As the law enforcement arm of the Department of State, DS is responsible for upholding the integrity of the U.S.

visa and passport through enforcement of relevant portions of the United States Criminal Code. DS is the most geographically extensive Federal law enforcement agency in the United States Government, with approximately 1,400 Special Agents dispersed among 25 field and resident offices domestically, with representation on 26 Joint Terrorism Task Forces, and with assignments to U.S. embassies and consulates in 159 countries. DS is uniquely positioned and committed to meet the serious national security challenge of travel

document fraud. Our agents conduct investigations into passport and visa fraud violations wherever they occur. Our partnership with the Bureau of Consular Affairs has enabled us to jointly focus on protecting the U.S. passports and visas.

Overseas, we work with foreign partner nations to target and disrupt document fraud rings and human smuggling networks. Domestically, we work with local, State, and Federal law enforcement agencies to investigate, arrest, and seek prosecution of fraud violators. Throughout this global network of law enforcement professionals, DS Special Agents are on the front lines of combating terrorist and criminal travel.

Terrorists targeting the U.S. attempt to discover, manipulate, and exploit vulnerabilities within our travel document system. To successfully counter this threat, DS has crafted a Visa and Passport Strategic Plan that leverages our international expertise and worldwide presence. The plan provides the framework for a Visa and Passport Security Program and will significantly augment the Department's ongoing efforts to prevent terrorist travel. Our approach incorporates the principles of the National Strategy to Combat Terrorist Travel and the objectives of the Intelligence Reform and Terrorism Prevention Act of 2004.

The Strategic Plan requires the deployment of additional DS personnel to critical posts worldwide, resources to enhance our intelligence and data-sharing efforts, and training and technical assistance to our foreign partners. Presently DS Special Agents assigned to consular sections abroad focus solely on travel document fraud. By the end of this year, DS will have 33 Special Agents assigned to key posts investigating document fraud. By the end of 2008, we will have 50 agents in this capacity. Since 2004, the results have been promising, yielding nearly 1,050 arrests for document fraud and related offenses, in excess of 3,400 visa refusals and revocations, and more than 6,200 foreign law enforcement and security personnel trained.

The plan is built on a cornerstone of three strategic goals: to defend the U.S. and our foreign partners from terrorist attack through aggressive, coordinated international law enforcement actions and initiatives; to detect terrorist activity, methods of operation, and trends that exploit international travel vulnerabilities; and, lastly, to disrupt terrorist efforts to use fraudulent travel documents through strengthening the capabilities of our foreign partners by such highly successful programs as the DS' Anti-Terrorism Assistance Program.

Our Strategic Plan offers a comprehensive and proactive approach to ensuring the integrity and security of U.S.

passports and visas.

Thank you for the opportunity to brief you on this vital aspect of DS's mission. I look forward to answering your questions.

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

Chairman FEINSTEIN. Thanks, Mr. Donovan.

Mr. Everitt?

**STATEMENT OF MICHAEL P. EVERITT, UNIT CHIEF, FORENSIC DOCUMENTS LABORATORY, IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.**

Mr. EVERITT. Good morning, Chairman Feinstein, Ranking Member Kyl, distinguished members of the Subcommittee. I am pleased to be here today to discuss strengthening the security of international travel documents to prevent terrorist travel. The U.S. Immigration and Customs Enforcement Forensic Document Laboratory is dedicated exclusively to fraudulent document detection and deterrence. The FDL is accredited by the American Society of Crime Lab Directors-Laboratory Accreditation Board (ASCLD/LAB) in questioned documents and latent prints and enjoys a worldwide reputation for excellence in the detection and identification of fraudulent travel and identity documents.

The FDL provides a wide variety of forensic and support services to all Department of Homeland Security components, including ICE, CBP, USCIS, the Secret Service, and the Coast Guard. The FDL also supports all Federal, State, and local agencies, as well as foreign government law enforcement and border control entities upon request. The FDL is an integral part of a comprehensive approach to disrupting terrorist travel and works both domestically and internationally to strengthen the security of international travel documents.

The FDL is like many other forensic laboratories in that it has a cadre of highly trained and experienced forensic scientists and support staff who conduct forensic examinations. These FDL employees make up the Forensic Section of the FDL and include forensic document examiners, physical scientists, ink chemists, fingerprint specialists, forensic photographers, and seized property specialists. This team of experts processes over 5,000 submissions each year.

The training requirements for the forensic section positions are rigorous. As an example, before conducting their first solo examination, forensic document examiners must successfully complete an in-house, 30-month, full-time training program. Comprehensive training programs such as these are necessary to acquire and maintain laboratory accreditation and personal certification.

The FDL differs from most forensic laboratories in that it also has a separate group of employees who collect and analyze information developed by the Forensic Section about fraudulent documents and distributes that information to the field via publication, real-time support, and training. These employees are senior intelligence officers that make up the Operations Section of the FDL. Many of the senior intelligence officers working at the FDL have previously worked at large ports of entry and have extensive experience with international travelers and the documents that they use.

Operations Section personnel provides real-time support to field personnel throughout the world with questions about suspected documents. These personnel include Department of State consular officers adjudicating visa requests, USCIS personnel adjudicating requests for immigration-related benefits, and ICE and CBP personnel working in the field and at ports of entry and other Federal,

State, and local law enforcement officers. In fiscal year 2006, the FDL received over 5,200 inquiries of which more than 2,400 were from non-DHS agencies.

Publications produced by the Operations Section include Document Alerts, Intelligence Briefs, and Reference Guides. These publications are printed and distributed to more than over 800 law enforcement and border control agencies worldwide to assist officers in identifying fraudulent documents. Many of these documents are also posted on DHS Internet portals to make them available to other law enforcement entities.

Senior intelligence officers also design and provide fraudulent document recognition and training programs for DHS personnel and other Federal, State, and local law enforcement officers. This fiscal year alone, the FDL has trained more than 1,900 individuals in locations around the world, including the United States, South Africa, El Salvador, Botswana, Jordan, Trinidad and Tobago, Kenya, Turkey, and Yemen. Much of this training is in support of Department of Homeland Security, Department of Justice, and Department of State initiatives. The FDL also receives requests for training from State and local law enforcement and from private concerns.

The problem of fraudulent documents is a perplexing one. The wide availability of technology to create high-quality fraudulent documents demands that the producers and issuers of legitimate documents develop and use new security features and production techniques that cannot easily be duplicated. Many new security features and production techniques have been developed; unfortunately, they are not always used in many travel and identity documents issued in the United States and other places throughout the world.

Travel and identity document producers and those who issue legitimate documents are in a constant battle to develop new production and security features and make travel and identification documents more secure. We try to assist in that and providing counterfeit deterrence studies to those who produce travel and identity documents.

It is important to understand that fraudulent travel and identity documents are not only a challenging problem for the United States, but for law enforcement officials throughout the world. As long as identification is required to travel and obtain services, criminals and terrorists will attempt to produce fraudulent documents. The ICE FDL will continue to work diligently to combat the production and use of fraudulent documents through our efforts in document examination, the development of higher-quality documents, and the training of law enforcement and border control officers throughout the world.

On behalf of the men and women of ICE, and specifically the men and women of the Forensic Document Laboratory, who are the country's subject matter experts on travel and identity documents, I thank the Subcommittee and its distinguished members for your continued support. I would also extend an open invitation to members to visit the ICE Forensic Document Laboratory as I believe you would find the visit both interesting and enlightening.

I would be pleased to answer your questions at this time.

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

Chairman FEINSTEIN. Thank you very much, Mr. Everitt.

Because Senator Kyl has to leave, he would like to ask you a couple of questions.

Senator KYL. I just have one main question, and I will try to submit written questions to the rest of you. But with proper training, could a person detect the counterfeiting of a U.S. passport if that passport has been screened into a computer from an off-site computer to, let's say, a DHS office here in Washington?

Mr. EVERITT. I am sorry, sir. I am not sure I understand your question.

Senator KYL. You take the passport in Omaha, Nebraska, and you screen it into a computer, which is connected to DHS.

Mr. EVERITT. Yes.

Senator KYL. A trained individual looks at that computer screen with the passport on it. Can you detect—to what degree of certainty could you detect a counterfeiting of that U.S. passport?

Mr. EVERITT. That is a service that actually the FDL provides through real-time support. What we would do then is we work—it is not a matter of us just looking at that scanned image. We would be on a two-way communication with that person. We are looking at the image. We are asking them questions—Do you see this? Do you see that?—looking for specific security features in the document.

That two-way transaction, oftentimes we can help them make a determination, which is a probable cause determination, of whether or not that document is valid or not.

Senator KYL. Excuse me. How trained would the person on the transmitting side have to be?

Mr. EVERITT. Basically trained enough to have the initial suspicion that the document was bad.

Senator KYL. Let us assume that this is simply being used to determine something like eligibility for employment and there is no training involved, but simply an individual who is putting it on a computer screening device to transmit to, let's say, the Department of Homeland Security for a determination of validity, and you have the basic information typed in, but then you are looking at the photograph and other features on it.

Mr. EVERITT. They would have to at least have some cursory amount of training to understand what we are asking, the questions that we are asking them. In other words, they would have to understand what a hologram was or what a kinegram—not the technical aspects of those, but at least to know what we are referring to or what we are asking them to look at.

Senator KYL. What would be involved in that cursory amount of training?

Mr. EVERITT. It is training that we do that can last anywhere from 4 hours up to a couple days.

Senator KYL. So it would be impractical if every employer in the country were required to do this, to assume that they could be adequately trained for this to work, for this to provide some high level of confidence that you can detect a fraudulent passport?

Mr. EVERITT. It would require some pretty extensive training, yes, sir.

Senator KYL. OK, just by the simple mechanism of screening it into the computer.

Mr. EVERITT. Yes, sir. Using that process, yes, sir.

Senator KYL. Because you use a specifically designed piece of equipment at the ports of entry for—or do you? Let me ask that question. Is this strictly a visual thing with the inspectors? Or is there a piece of equipment that is used?

Mr. EVERITT. It is a visual examination of the document. The equipment that is used is a reader that is reading the machine-readable zone, the MRZ.

Senator KYL. Right.

Mr. EVERITT. And then is making queries against databases based on that information.

Senator KYL. OK. Good. Thank you very much.

Mr. EVERITT. You are welcome.

Chairman FEINSTEIN. Thank you very much, Senator.

Mr. Morris, would you like to proceed?

**STATEMENT OF PAUL MORRIS, EXECUTIVE DIRECTOR, ADMISSIBILITY REQUIREMENTS AND MIGRATION CONTROL, OFFICE OF FIELD OPERATIONS, CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.**

Mr. MORRIS. Good morning, Chairman Feinstein, Senator Kyl. I am very pleased to be here today to discuss how the Department of Homeland Security, particularly U.S. Customs and Border Protection, is moving forward on programs that will facilitate travel, but still provide the level of security required to protect the United States and, of course, interrupt terrorist travel. This is an enormous challenge. We share more than 7,000 miles of borders with Canada and Mexico and operate 325 official ports of entry. Each year, CBP front-line officers inspect more than 422 million travelers through official land, air, and sea ports of entry.

I begin by expressing my gratitude to the Subcommittee for the support you have shown for important initiatives that enhance the security of our homeland. Your continued support has enabled CBP to make significant progress in effectively securing our borders and protecting our country against terrorist threats.

DHS is committed to working with Secretary General Noble of Interpol on the implementation of the Stolen Lost Travel Document (SLTD) system this year. CBP has taken the lead in the implementation of this program, and we are currently on schedule to become the first major country to use the SLTD as an integrated prescreening tool.

Since its inception on March 1, 2003, CBP has worked diligently to facilitate the flow of legitimate travelers into the U.S. A small percentage of travelers, however, attempt to enter the U.S. illegally through the use of fraudulent documents or other fraudulent means. In response, CBP has implemented a number of complementary programs, both domestically and internationally.

The standardization of travel documents is a critical step to securing our Nation's borders. Currently, travelers can present thou-

sands of different documents to prove their citizenship when attempting to enter the U.S. The Western Hemisphere Travel Initiative (WHTI) requires all travelers to present a passport or valid travel document to enter the U.S.

The initial phase of WHTI went into effect January 23, 2007, obligating all air travelers to present a passport or other acceptable secure document for entry to the U.S. The implementation of the air portion of WHTI was highly successful, with documentary compliance rates of 99 percent and no interruption to air transportation.

As early as January 1, 2008, travelers arriving by land or sea will be required to present a valid passport or other secure document, as determined by DHS, working with the Department of State.

US–VISIT uses biographic and biometric information to enhance the security of U.S. citizens and visitors. Biometric data obtained overseas when the Department of State issues a traveler's visa is verified with the biometric data collected at the port of entry, confirming that the individual applying for admission is the same person who was granted the visa. Biometrics protect our Nation and our visitors by making it virtually impossible for anyone else to claim their identity should their travel documents, such as a visa, be stolen or duplicated.

Each year approximately 15 million people from designated Visa Waiver Program, or VWP, countries enter the U.S. free to travel for 90 days without a visa. In an effort to provide for secure verification of passport validity and to better detect fraudulent passports from VWP countries, e-passports were mandated for participating countries in October 2006. These e-passports, which have an embedded electronic circuit chip—similar to the one used by the U.S.—contain biographic and biometric data, and they assist CBP front-line officers in detecting fraudulent passports and passports in which the photograph was substituted or altered.

In a continuing effort to extend our zone of security outward, the Immigration Advisory Program (IAP) posts officers overseas at high-volume, high-risk airports to screen passengers before they board aircraft destined for the U.S. Since the IAP became operational, more than 1,624 passengers have been prevented from boarding planes bound for the U.S. Current IAP locations include Amsterdam, Warsaw, London-Heathrow, and Tokyo-Narita.

Additionally, the Carrier Liaison Program was developed to enhance our border security by helping commercial carriers to become more effective in identifying improperly documented passengers destined for the U.S. And in December 2006, we established three Regional Carrier Liaison Groups that provide 24/7 points of contact for carriers and assist them in making recommendations not to board aliens identified as fraudulently or improperly documented. These RCLGs in fiscal year 2007 so far have denied boarding for 419 improperly documented travelers, 150 of whom were carrying fraudulent documents.

In January 2005, we established the Fraudulent Document Analysis Unit to collect documents, provide ports with analysis of document trends and intelligence information, and target persons being smuggled into the U.S. using fraudulent documents.

In addition to those initiatives, we have been working in four areas to improve the data CBP gathers and maintains on lost and stolen passports:

First, we have been refining the use of targeting systems to search for "near misses" to account for alterations of passport numbers by forgers attempting to defeat the watch listing of lost and stolen documents.

We are currently accessing the Interpol SLTD, and as we continue that work with Interpol, we will increase our ability to access that information in different ways.

We are working with Australia and New Zealand on the Regional Movement Alert System pilot, and this is a trilateral pilot that enables participating countries to access data on lost, stolen, and otherwise invalid travel documents in real time.

And we are working to become the first point of intake for all lost and stolen passport information to the U.S. This would ensure that this critical data is immediately directed to the border screening system.

Chairman Feinstein, Senator Kyl, I have outlined today some of the ways that CBP and DHS, working with our key partners, detect and intercept fraudulent documents at or before the border, while facilitating legitimate trade and travel. I appreciate this opportunity to testify and would be happy to answer any questions you may have.

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

Chairman FEINSTEIN. Thank you very much, Gentlemen. I appreciate it.

I would like to refer you, Mr. Morris—and you will have to just take these numbers down and read it—pages 11, 12, 13, and 14 of the transcript from a hearing held in this Subcommittee on September 7, 2006, and the Homeland Security witness was special counsel Mr. Rosenzweig, and I asked some questions, and I would like to quickly go over them. And I am talking about a GAO report here that has been done on the Visa Waiver Program, and it says, "It also recommends that DHS develop and implement a plan to make Interpol's stolen travel document database automatically available to immigration officers at primary inspection points."

And then we go on to, "What four countries do not share lost or stolen passport information with Interpol?" And the countries at that time are Holland, Japan, Norway, and Sweden.

And then I would like to quote to you Mr. Rosenzweig's testimony. "My goal would be to have the operational difficulties 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." And then I say, "Of 2006? I am writing it down, and I am going to get you to sign it afterwards."

Rosenzweig: "Absolutely."

Feinstein: "Operational when?"

Rosenzweig: "My goal is the 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," and he goes on: "...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."

Now, I have been trying on and on and on to get a time for a real-time Interpol connection, and here we have testimony that it will be in place by the second or third quarter of this year. My question: Will DHS meet this goal?

Mr. MORRIS. I believe that we will, Senator. We—

Chairman FEINSTEIN. So your answer is "yes, I believe," or "yes"?

Mr. MORRIS. We are currently designing the system within Interpol. We intend to test the system in early fall of this year, and we will have a pilot test at a major U.S. international airport in place shortly thereafter. Immediately after that brief pilot test, we intend to have a rapid deployment to the balance of our border control system.

Chairman FEINSTEIN. Well, I will be asking Mr. Noble these questions, but I assume—let me try and extrapolate what I hear from that. There will be a pilot test by the second or third quarter of this year. That pilot test will go on for how long?

Mr. MORRIS. Approximately 30 days.

Chairman FEINSTEIN. Thirty days, and then after the 30-day period, a full system will be put in place. And that will take how long to put in place?

Mr. MORRIS. If the pilot is successful and we are able to address any issues or concerns that may arise at that point, it should be a rapid deployment.

Chairman FEINSTEIN. And what does that mean?

Mr. MORRIS. That as soon as we can put the system in place, it will be in place.

Chairman FEINSTEIN. Well, are we talking about 1 month, 6 months, a year?

Mr. MORRIS. Without knowing what the success of the pilot may be at this point, I would say it would be much more rapid than that. We are hoping for immediate implementation after the pilot if the issues can be addressed.

Chairman FEINSTEIN. I guess my problem always is hope, you know, goal, and generally no time deadline is ever kept. So I really hope this is an exception because I really believe the security of our Nation is at stake. And I think this is a very worthwhile program.

Mr. MORRIS. And we agree 100 percent, Senator. And perhaps I should correct my statement and say that we expect that it will be a rapid implementation immediately after the pilot is concluded.

Chairman FEINSTEIN. OK. I will have you back after the third quarter, and I will pull out this transcript of today and read it back to you, and hopefully we will be there.

Mr. MORRIS. Do I have to sign it, Senator?

[Laughter.]

Chairman FEINSTEIN. With that understanding. All right.

If I might ask a question, and then I see we are joined by Senator Schumer, and he wants to make a statement and ask some

questions, so I will turn it over to him. The two passports, Mr. Simkin, that you gave us, one of the passports looks like the face page is embossed onto the passport. Is that correct? And that is the passport of Allen Ethan, or Ethan Allen.

Mr. SIMKIN. This one is an emergency photo digitized passport. This is the new system for issuing passports in emergencies at our posts overseas, and it is actually printed on a sticky foil that is then placed in the passport book. And, yes, there are some security features there over the photo and over the biographic data.

Chairman FEINSTEIN. Is this a process that is easy for somebody to replicate?

Mr. SIMKIN. It is not easy to replicate.

Chairman FEINSTEIN. But can it be replicated outside of the Government?

Mr. SIMKIN. We are not aware of any successful attempts to replicate this at this point. Of course, there are people always trying to duplicate our documents, so it is a constant effort to stay ahead of those efforts.

Chairman FEINSTEIN. Right. Well, I have a relatively new passport, and it has a chip embedded in it.

Mr. SIMKIN. Yes.

Chairman FEINSTEIN. And the face page is very different than these face pages.

Mr. SIMKIN. Is it similar to the model—

Chairman FEINSTEIN. It is blue. It is a regular—yes, it is not an official passport. So I am puzzled by this. It is a much thicker page, and I thought all new passports were being done that way.

Mr. SIMKIN. This exemplar is the current exemplar, and it is the only one that has the chip in it.

Chairman FEINSTEIN. Which one is that?

Mr. SIMKIN. The one with the symbol on the cover with the two bars and the circle in the middle.

Chairman FEINSTEIN. Right. All right. So this has a chip in it?

Mr. SIMKIN. Yes.

Chairman FEINSTEIN. And this, too, is blended onto the page. I guess—

Mr. SIMKIN. Yes, in this case it is printed on this page. It is not on a foil that is stuck into the passport. And then it is protected by a crystogram, and it is hard to tell, but we have actually an image of the U.S. Capitol in the center of the crystogram, an image of George Washington in the upper right, which make it difficult to alter or forge.

Chairman FEINSTEIN. Yes. I do not see either of them, but—Mr. Simkin. I found it hard in this light. You sort of have to-Chairman Feinstein. Right.

Mr. SIMKIN. Yes.

Chairman FEINSTEIN. OK. One other question. Mr. Everitt, today there is no law that prohibits the trafficking in ten or more passports or other travel documents. And one of the things I have learned from reading intelligence is that within visa waiver countries, there are large numbers of stolen passports, Geneva Convention travel documents, international driver's licenses.

In your experience, has the number of document mills that produce false documents for sale been increasing?

Mr. EVERITT. It is hard to say whether they have been increasing or not. There has always been a large number of document mills for producing fraudulent documents. It is one of those things that you do not know they are there until you find them.

I can say that there is a huge number of fraudulent documents circulating throughout the world.

Chairman FEINSTEIN. What effort is made to round up the stolen passports that are stolen—and I cannot mention the countries, but they are European countries—by the thousands? What effort is being made to secure those documents?

Mr. EVERITT. Well, I think that all the countries, just like us, you know, have investigative elements that are out there looking for these documents, trying to find them whenever they can. And, of course, anytime that these documents are encountered at ports of entry or exit, whether it be in Europe or in the United States, they are immediately seized.

We get reports on a fairly consistent basis of these documents—

Chairman FEINSTEIN. Do we have the methodology to be able—let's say a Central European country experienced a large theft of counterfeit-proof passports and it is a visa waiver country, and that passport can be bought by someone who would do us harm, who comes into this country with the passport from a visa waiver country. What is being done to see that that does not happen?

Mr. EVERITT. Well, hopefully the country that had the passports stolen would report those to Interpol. Those numbers would then be transmitted to CBP through the National Targeting Center. That information is passed amongst all the different types of entities. Lookouts are placed for them, and then hopefully when that person attempts to use that passport, it will be interdicted and they will be stopped.

Chairman FEINSTEIN. Well, I would be curious, then, because I have sent your agency the intelligence report on the theft, and I would be very interested in knowing exactly what action was taken, if any. So might I ask you that question, and we will follow that up with a letter as well.

Mr. EVERITT. Yes, ma'am.

Chairman FEINSTEIN. OK. Thank you.

Senator Schumer, thank you for joining us.

## STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Well, thank you, Senator Feinstein. I want to thank you for holding a very important hearing. Securing international travel documents is a critical building block of the larger project of border security. And as a representative of a border State, like Chairman Feinstein, I fully agree with her. We need security and efficiency at our international borders. We need both.

My question today is going to focus on a specific travel document, the so-called PASS card, People Access Security Services card. As everybody is probably aware, this is the card Department of State and Homeland Security are proposing to issue to travelers as part of the Western Hemisphere Travel Initiative. I am very dubious of the PASS card. I have serious questions about it. Again, I think that in a certain sense it is bureaucracy at its worst, taking an

overall solution that has worked in other places and not looking at how it works when you go across the border, that people travel from Fort Erie, Canada, to Buffalo daily—every day back and forth—and they do not get passports. They do not apply in advance to travel. It is expensive and will really hurt commerce.

At the same time, I have some privacy concerns, and I am disappointed that Homeland Security once again, instead of trying to be creative and find a solution that both will deal with our security needs as well as the travel back and forth, does not try to do that. And they say, well, passports work when you fly from Detroit to Munich; therefore, they can work when you go from Hamilton, Ontario, to Detroit. It is just different, and we are not looking at that.

I am really troubled by everything about it, and one would hope that we would have an executive branch that would deal with the problems, the unique problems that citizens have in Washington State, in North Dakota, in Michigan, in New York, in Maine, instead of just saying we are going to try to shove this round peg through a square hole, call it by a slightly different name, and not deal with the problems that it will create, or, oh, they will adjust to it.

What if people do not? What if commerce across the Niagara River slows down by a third and the economy, which is tough enough in wester New York, plummets?

So I am disappointed, I have to say. I want security. I do not want to back off on security. I would prefer not to delay anything—but not if we just get these kinds of answers, which I think we have gotten, Madam Chairman, throughout the whole system.

So that is where my questions are aimed. I am worried about the PASS card because of the inefficiencies, without the security. In a sense, we are getting the worst of all worlds. And when I say security assurances, I am concerned both about the security of the borders and about the privacy and security of individuals' personal information.

DHS has said they want to require these passports in January 2008—that is pretty soon—even though the final deadline is not until June 2009, about 18 months later. Yet we have yet to see a regulation, a final regulation on the WHTI or on the proposed PASS card. So there are a whole lot of unanswered questions, and it is supposed to be less than 6 months away. It is mind-boggling.

I hope we will get the answers soon, maybe even in a few minutes. In the meantime, we have to deal with the issue.

The State Department has said it will process PASS cards just like passports, but it is now a 10-week wait for a passport. Are we going to have a 10-week wait for somebody who learns of a wedding, say, and wants to go across the border in 6 weeks? Or for a school bus, a bunch of school kids that want to go look at something in Buffalo and they are from Canada? It is going to change the whole way of life because the Niagara River is not unlike the Hudson River in the sense that people cross it regularly, day by day, and that is true in Detroit and it is in true in Washington State and it is true in Maine. It is true in other parts of New York State.

So, I do not know, I just do not see the concern here. We need to be careful that we are maintaining efficiency and protecting security. And I hope this hearing will advance the cause.

So my questions are mainly directed at Paul Morris and Andrew Simkin of DHS and State. First, you said you want to use radio-frequency vicinity-read technology in the proposed PASS card. That is not the most secure technology available for this type of card. The PASS cards lacks many of the security features that are possible for, say, the e-passport. However, State and DHS have claimed that the proposed PASS card technology will be more efficient. I appreciate and agree with the goal, but I want to look behind the claim that the PASS card would both be secure and efficient, that it would let us have our cake and eat it, too.

So my question to you two gentlemen is: The proposed technology for the PASS card is different from the technology used for existing U.S. border documents like e-passport and Nexus registered traveler card, right? I assume that is correct. Yes?

Mr. SIMKIN. Well, the technology is actually still subject to some testing and analysis before a final decision will be made. But the proposal is, yes, it would be vicinity-read.

Senator SCHUMER. All right. Now, Mr. Morris, if you disagree with any of that, you can chime in. But you agree it is different, I presume. OK. Given this specific technology has not been used for U.S. travel documents before, have the proposed PASS cards themselves been field tested in a real border environment?

Mr. SIMKIN. No.

Senator SCHUMER. No. And we are supposed to have this fully implemented in 9 months, right?

Mr. SIMKIN. Well, actually the time range could be as early as January 2008 by law, or it could be as late as June of 2009.

Senator SCHUMER. OK. And you do not have a set date yet by which you will be ready?

Mr. SIMKIN. We do not have a set date.

Senator SCHUMER. OK. What about the machines to read the PASS cards? Has DHS or State done any field test of these cards readers, Mr. Morris?

Mr. MORRIS. Well, it comes down to the final technology that is selected for the card and testing in conjunction with that. We have done some field testing of various technologies. It is certainly in general a viable technology. The final solution, we will have to take a look at it.

Senator SCHUMER. But the type you aim to use has not been tested yet in the field?

Mr. MORRIS. That is correct, sir.

Senator SCHUMER. OK. So you have stated, both State and DHS, that PASS cards will be readable at 20 feet away as a car approaches the border crossing. Is that a guess? I mean, do we know when there is a traffic stream with different lanes and different cars going back and forth that it will work 20 feet away?

Mr. SIMKIN. The passport card is an alternate to the paper passport. As you know, we have a proposed rule, and I know that you submitted comments, and many of your constituents did. Those comments are being evaluated now prior to the issuance of a final rule, and it is a joint State and DHS effort.

We are committed to working closely with the National Institute of Standards and Technology to ensure that whatever technology goes into the card is a workable one.

Senator SCHUMER. Yes, but we do not know if it is readable at 20 feet yet. We have not done an on-the-ground experiment yet or—

Mr. SIMKIN. It is going to require extensive testing.

Senator SCHUMER. It is? OK. So we have not done that yet.

OK. The current plan also requires CPB to have a database that will store and pull up personal information based on the PASS cards. That database would be a gold mine for identity theft thieves and terrorists. What testing has been done to make sure the database is protected from hackers and from physical attacks? Because it is going to be in a lot of places, I guess, or accessible in a lot of places. Mr. Morris?

Mr. MORRIS. As with all of our systems of law enforcement information, they are appropriately firewalled, appropriately secured to ensure that none of the Privacy Act-protected information is going to make it into the hands of anyone but those that need it and have appropriate access to the—

Senator SCHUMER. Well, that is a general hypothetical statement. What specific plans have been done, put in place? I mean, you are saying you are going to implement it as early as 8 months from now or 7 months from now. What practical steps have been taken, what tests have been done, to make sure that it cannot be—that identity thieves cannot prey on this?

Mr. MORRIS. I would have to take that back as a question for the record, sir.

Senator SCHUMER. OK. If we could by unanimous consent, I would be happy to get an answer in writing. In a week?

Mr. MORRIS. Certainly.

Chairman FEINSTEIN. So ordered.

Senator SCHUMER. Thank you.

So it is a real concern that the proposed PASS card will be just as inconvenient and inefficient at busy border crossings as a passport book and will be a double whammy because it provides less security than the new e-passports. And I do not see a change here. Let me just ask a couple of other questions.

What is your answer to the 10-week backlog that we now have with passports given the needs that people have right away, given the fact that only 7 percent—I get the numbers mixed up. It is 7 percent of either Canadians or Americans have a passport and 9 percent of the other, at least in the western New York area.

Mr. SIMKIN. OK. Nationally, we believe it is about 27 percent of American citizens hold passports at the present time. That is going up. As a result of the Western Hemisphere Travel Initiative, we have seen a very strong surge in passport demand. Last year, we issued a record 12.1 million passports. This year, we are on track to issue over 17 million passports. We have all of our passport agencies working extra shifts, working mandatory overtime. We have task forces operating in Washington.

We have not been able to get the delay down to where we would like it to be. We are committed to following the rigorous adjudica-

tion processes to make sure that we only issue passports to persons entitled to them.

Senator SCHUMER. So what do you say to somebody, if this plan were in effect, who gets an invitation to a party, to a wedding, to something on the other side of the border 3 or 4 weeks from now and they do not have a passport?

Mr. SIMKIN. We take a lot of steps to try to accommodate emergency situations. We have walk-in service at most of our agencies. We have an expedited service that can cut that time down considerably from 10 weeks.

Senator SCHUMER. Have you made any plans to improve things on the border areas so we will not have long waits, so that people who on the spur—I mean, this does not even deal with the issue, about a quarter of the fans, for instance, who see the Buffalo Sabres are Canadians. I bet a lot of them decide to go that day. Now, are there plans to deal with these kinds of things? Let us take something that is not just a hockey game. Let us say, you know, there has to be a business meeting, there has to be a serious gathering of different people for one thing or another—a funeral.

Mr. SIMKIN. Well, it is a legal requirement under the Western Hemisphere Travel Initiative, under the IRTPA legislation. We are trying to do everything we can to provide the best customer service to enable people to travel in the time that they wish to. We get hundreds of thousands of calls, and many of those calls we can prioritize the passport application for short-term travel. We can also route people to walk-in counter service to be able to try to meet their travel needs.

Senator SCHUMER. Walk-in counter service? Do you have plans to open up lots of these walk-in counter places throughout western New York and throughout eastern Canada by January of 2008? Do you have any plans for that?

Mr. SIMKIN. No.

Senator SCHUMER. OK. I mean, my questions are pretty obvious here in terms of where we are going.

You would both agree that if there is a 6-week wait to get—let's say it is not 10 weeks, it goes back to 6—a 6-week wait before anyone could travel across the board, that would greatly hurt commerce along the whole Northern border dramatically and hurt the economy significantly? Do you agree with that? Yes or no.

Mr. SIMKIN. I am really not an expert in commerce. It is obvious that there is an inconvenience factor to this—

Senator SCHUMER. No, no, no. I did not ask inconvenience. That belittles it. A serious economic effect.

Mr. SIMKIN. I really could not say what the effect is. I am not aware of any studies of what the effect would be.

Senator SCHUMER. Isn't it common sense that if people who are used to traveling across the border in a totally different way now have to wait 6 weeks before they travel?

Mr. SIMKIN. One thing I would point out with regard to the documents required for entry to the United States, this is a requirement that is levied at the port of entry. State and DHS work together on these things. Our job in the State Department is to issue the passports properly to people entitled to them in as fast and efficient a way as we possibly can.

Senator SCHUMER. Now there is a 10-week wait.

Mr. SIMKIN. Correct.

Senator SCHUMER. That is not very fast.

Chairman FEINSTEIN. Senator, if I may?

Senator SCHUMER. Yes.

Chairman FEINSTEIN. If you could truncate—

Senator SCHUMER. I am almost finished.

Chairman FEINSTEIN. Because we have got another panel.

Senator SCHUMER. OK. You agree, Mr. Morris? What is your view? Would a 6-week or a 10-week wait interfere with commerce across the Northern border from Seattle over to Presque Isle, or wherever the eastern order of Maine is?

Mr. MORRIS. I think I would have to suggest, Senator that stating that it is a 6-week wait is perhaps not entirely accurate.

Senator SCHUMER. No, but if it were. If it were.

Mr. MORRIS. Well, we have launched a significant media campaign to make individuals aware of the current requirement for air travel. We are going to continue that to make any individuals aware of the land border and seaport requirement as well. Our hope would be that they would plan in advance to get the passport that they need so that there is no interruption in their travel when the actual requirement is put in place. And for those—

Senator SCHUMER. There are certain things you cannot plan for, right? Funerals, emergencies, business meetings.

Mr. MORRIS. That is true, and within Customs and Border Protection's discretionary authority, we can address those types of cases on a case-by-case basis as they arise.

Senator SCHUMER. OK. I would just say—and I just have one more. I know you want to move, Madam Chairperson. I mean, we work with both of your Departments on these case-by-case bases, and sometimes it works out and sometimes it does not. And all of us have dealt with this because we get calls from our office regularly, and I would urge you to give more thought to this and not just treat it as business as usual or say, "We will work it out on a case-by-case basis," because if this is implemented and then it creates a real problem, you all know that it is going to be worse than if it is—well, it is going to create huge problems.

Just one more question. Many of us like the idea of using driver's licenses, the special new driver's licenses, as a better way to do this. It is a document people are familiar with. It is more inconvenience to you, less problems for the people at the border. Washington State is doing a pilot project in this regard. Can you tell us how it is going?

Mr. MORRIS. I can tell you, Senator, that we have been actively engaged with the State of Washington in looking at this particular pilot. We would be happy to provide you more information through a—

Senator SCHUMER. You are not familiar with it right now?

Mr. MORRIS. No, I am not, sir.

Senator SCHUMER. OK. Please, if you would. That is very important.

Mr. MORRIS. Certainly.

Senator SCHUMER. And I would urge you to look at alternatives like the driver's license alternative, which, as you can imagine,

most everyone has a driver's license, they are used to a driver's license, they do not have to apply in advance, they do not have to pay, they have it anyway. I would urge you to look at that rather than sort of stick to business as usual, which does not quite work for our border.

Thank you, Madam Chairperson.

Chairman FEINSTEIN. Thank you, Senator.

Before I close out the panel, I would like to bring to their attention an article on the front page of the New York Times this morning, and that is the article entitled "U.S. Seeks Closing of Visa Loophole," by Jane Perlez. And it points out that the head of the London bomb attack actually has a passport through the Visa Waiver Program and could have come to this country at any time under the Visa Waiver Program.

I truly believe that the Visa Waiver Program is the soft underbelly of this Nation. The predominance of stolen passports makes it so easy and there are so many countries in the Visa Waiver Program. I just want to quote a part of it. "Among the options that have been put on the table, according to British officials, was the most onerous option to Britain, that of canceling the entire Visa Waiver Program that allows all Britons entry to the United States without a visa."

I think—and I have been following this program closely for some amount of time—that the way it is run and the sloppiness with which it has been run really places this Nation in serious jeopardy. And I have said this over and over and over again. I was the one who fought against getting rid of the 3 per cent visa refusal rate for countries that want to participate in the program. I think we have a big problem there in that millions of people come in, well over 15 million people a year, essentially on a program where there is no check and no balance. And I would just like to leave you with those thoughts. And I think we are going to have much more to say about it in the future.

So thank you very much for your testimony this morning. It is appreciated, and if you gentlemen have a chance to stay to listen to Mr. Noble, it might well be edifying.

Chairman FEINSTEIN. I would like to ask the second panel to come forward: the Honorable Ronald K. Noble, the Secretary General of Interpol; Clark Kent Ervin, Director of Homeland Security, Aspen Institute, former Inspector General, Department of Homeland Defense, and Author, "Open Target: Where America Is Vulnerable to Attack"; and also Brian Zimmer, Senior Associate, Kelly, Anderson & Associates, and former Senior Investigator, Committee on the Judiciary, United States House of Representatives.

If we can, we will begin with Mr. Noble, and let me thank you so much for coming here. It is very much appreciated. And I think you can note from my questions the interest that I have in the subject, and so I would very much appreciate your comments, if you can, addressing these points.

## STATEMENT OF HON. RONALD K. NOBLE, SECRETARY GENERAL, INTERPOL, LYON, FRANCE

Mr. NOBLE. Thank you very much. Chairman Feinstein, distinguished members of the Subcommittee, good morning. I will broad-

en the focus of my oral testimony to lay the foundation for why urgency should be felt by us all as we deal with the issue that brings us together today.

Al Qaeda and al Qaeda-inspired terrorists are trying to kill and harm the world's citizens. They are doing so right now. Depending on the group, the circumstances, and the opportunities, they would love nothing more than to kill U.S. citizens and the friends of U.S. citizens on U.S. soil. But they also love targeting U.S. embassies, U.S. military vehicles and personnel, U.S. businesses, and U.S. citizens anywhere—anywhere they might be found in the world. They know the combustible ingredients that attract worldwide attention. Al Qaeda strikes U.S. targets.

There are those who blindly take comfort that the U.S. has not been hit hard within its borders since September 11, 2001. I know one high-ranking U.S. Government official who was so dedicated and committed to protecting U.S. citizens on U.S. soil that on any given day he could tell you how many days it had been since September 11, 2001.

In my capacity as Interpol's Secretary General, I take no comfort, absolutely no comfort, in the fact that al Qaeda has not struck the U.S. within its borders since 9/11. Of course, we all should be thankful that no innocent lives have been taken or harmed. But viewing the absence of terrorist attacks on U.S. soil for a certain amount of time as a success is the wrong approach. And you talked about complacency earlier. It can give one a false sense of comfort, and it can make you falsely conclude that al Qaeda cannot strike as opposed to that al Qaeda has not yet chosen to strike.

For me, I use different points of reference in terms of time and comfort. I see the time since the last terrorist attack as a time bomb that must be defused before it explodes. My point of reference is not the number of days between September 11, 2001, and today, which happens to be 2,059, but the number of days between the first World Trade Center attack by al Qaeda on February 26, 1993, and the second set of attacks on September 11, 2001. Al Qaeda waited and prepared for more than 8 years, 3,119 days, before striking the U.S. again on U.S. soil.

This means that we cannot and should not take any real comfort from the fact that the U.S. has not been hit again since then. As I said, I use time bombs as my points of reference. I see members of al Qaeda, terrorists linked to al Qaeda, or individuals who are inspired by al Qaeda as human time bombs. They have almost 200 countries in the world where they can operate, whether they can plan or prepare and through which they can travel. The challenge for our generation and maybe for generations to follow is how can we individually and collectively prevent these vicious terrorists from killing or harming us and those we love and represent.

Since September 11, 2001, Interpol has been regularly transforming itself to help each and every one of its member countries to disrupt, to prevent, to investigate, to track down, to apprehend, and to prosecute terrorists the world over. We have done so by thinking about this issue almost every minute of every day, by meeting and consulting with our member country national central bureaus and law enforcement officials from around the world, by engaging elected officials, appointed Government officials, report-

ers, business leaders, and citizens in discussions about what they see as weaknesses in their countries' or even other countries' antiterrorist efforts.

The best way to describe Interpol's state-of-the-art approach to enhancing the border security of each and every country is to visualize tripwires interconnected around the globe and in the paths of terrorists and other dangerous criminals. Depending upon the type of tripwire that is tripped, either a silent or a loud alarm is triggered and alerting law enforcement that they might have a person of interest to another law enforcement agency somewhere in the world standing right in front of them, permitting them to move the person from primary to secondary inspection.

Interpol's tripwire system is in place and is working. Between 2000 and 2006, the number of annual checks on our databases increased nearly tenfold, from 81,000 to over 703,000. Between 2000 and 2006, the number of international wanted persons notices issued annually by us has nearly tripled from 1,000 to 2,800. The number of diffusions, or what we would know in the U.S. as Be On the Look-Outs, issued annually through Interpol has more than doubled from 5,000 to over 12,000. The number of annual arrests of individuals who were subject to Interpol Red Notices or diffusions has surged from 534 to over 4,000, a 698-percent increase.

Now, despite the success that Interpol and its member countries have achieved working together in terms of gathering and sharing information from a wide variety of countries on suspected terrorists, and especially on stolen travel documents, there seems to be an intractable resistance in some corners of the U.S.' and other countries' bureaucracies to using information coming from global sources. These entities prefer to use the systems that were in place prior to the first World Trade Center bombing in 1993 and prior to the September 11, 2001, terrorist attacks.

As I said in my written testimony, if this view continues to reflect the attitude of those whom we expect to protect us from the next wave of terrorist attacks, we are in serious—and I repeat—serious trouble.

Chairman FEINSTEIN. Would you be specific on that point?

Mr. NOBLE. Yes. If you were to read this morning's Wall Street Journal article regarding this hearing, you would see a quote given by the spokesperson from Customs and Border Protection saying that the Interpol system is not there yet, is not where it should be yet. And I believe this attitude courageously spoken on the record reflects the view of those people who remember Interpol 5 years ago or 6 years ago or 10 years ago when this was true. We have changed. The world has changed. We believe it is important for that to be recognized.

I will conclude with my formal remarks to say that, Chairman—and I say this with all sincerity—since you have organized these hearings, Interpol and our Stolen Lost and Travel Document database has gotten more attention from the U.S. than we received in my 6½ years as Secretary General—not that the U.S. has not been trying and has not helped us. In fact, it is for that reason that we have the system in place, because they complained about the old system that was only an investigative tool. So thanks to the feedback, the work of the USNCB, and the hard work of individuals in

U.S. Customs and U.S. Border. Now it is different. Progress has been made, but what I feel as Secretary General and the point I want to make is the time bomb, the ticking, your reference to what was promised last year, it will happen this year, we hope it will happen this year. But until it happens this year, there have got to be interim measures we can take.

When I was 9 years old working in my father's store, we used to have a book with the numbers of all the credit cards that were reported stolen or that were no longer valid that we would refer to. So what Interpol is saying, the perfect system may never be developed, but the system we have in place now that is being used by Switzerland over 300,000 times a month is coming up with 100 hits each month. The system that we put in place in the Caribbean before the Cricket World Cup, the Caribbean countries, whom people oftentimes criticize as not being aggressive or hard-working enough, put the system in place in 4 months and now have gotten more hits in 4 months than they got in the prior 6 years.

So we need the U.S. not only to put the system in place, but to advocate that other countries should put the system in place. Without the U.S. support, without the support of the elected Members of Congress, this Congress and other congresses and parliaments around the world, we believe people will take their time to make sure the system is put in place. And Interpol believes that time continues to run out for us.

Thank you.

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

Chairman FEINSTEIN. Thank you, Mr. Noble. I have many questions.

Mr. Ervin?

**STATEMENT OF CLARK KENT ERVIN, DIRECTOR OF HOMELAND SECURITY, ASPEN INSTITUTE, AND FORMER INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.**

Mr. ERVIN. Thank you very much, Chairman Feinstein, for inviting me to testify on this very important topic, and I want to thank you for being the leader on this issue of dealing with the Visa Waiver Program and the related problem of stolen and lost passports. As you know, I have submitted a lengthy statement for the record, so I will only summarize it here.

Like you, I believe that the single greatest vulnerability with regard to international documents is the Visa Waiver Program and, as I say, the inextricably interrelated problem of lost and stolen passports.

As we put it back in a 2004 report during my time as DHS Inspector General, "In the post-9/11 world the visa is more than a mere stamp in a passport. It is the end result of a rigorous screening process that the bearer must undergo before travel. By the end of the process, U.S. authorities have collected and stored considerable information about the traveler and his or her planned journey. When the visa is waived for broad classes of travelers, those travelers avoid this extensive examination, and the United States does not collect comparable information regarding them."

Visitors from non-visa waiver countries are nowadays almost always interviewed at an American embassy or consulate abroad about 90 percent. Many, if not most, of our interviewers are conversant in the language of the applicants, familiar with their customs, and trained in fraud detection techniques. Consular officials have the further luxury of spacing the interviews apart so as to maximize the time they have to question applicants.

By way of contrast, there is no time for port-of-entry inspectors to interview visa waiver travelers. Hundreds of passengers, as we all know, disembark at any one time from international flights, and, understandably, inspectors feel pressure to clear them within 45 minutes. And even if they did interview passengers, most inspectors speak only English. The relative few who speak another language tend to speak Spanish, not languages like Arabic, Farsi, or Urdu, spoken in countries of concern.

Far more written information is collected from non-visa waiver travelers than visa waiver travelers, and the finger scans taken at the port of entry from non-visa waiver travelers can be compared with those taken at the embassy or consulate where the visa application was made, establishing to a certainty that the person at the port of entry is the very same person who applied for the visa abroad.

It is not, then, for nothing that shoe bomber Richard Reid was a British citizen. It is not for nothing that Zacarias Moussaoui, whom some believe to have been the 20th 9/11 hijacker, was a French citizens. Terrorists prize passports from visa waiver countries because visa waiver travelers are subjected to much less scrutiny. That is why passports from visa waiver countries are occasionally stolen and used to attempt to enter the United States.

We do not know the full extent of this problem, but we do know that it remains a serious one. The latest figures that I am aware of are from January to June 2005, when, according to GAO, 298 stolen visa waiver country passports were used to try to enter the United States. We do not know, of course, how many times customs inspectors failed to spot stolen passports. At least when we looked into this problem back in 2004, we found, incredibly enough, that DHS customs inspectors admitted travelers with stolen passports into this country 73 percent of the time when they knew that the passports were stolen.

I want to take issue, if I may, with Mr. Everitt who said that it is invariably the case that when stolen passports are discovered by port-of-entry inspectors, they are confiscated. At least when we looked into this problem in 2004, on occasion, also incredibly, the passports were given back to the traveler so that he could go back to his country and attempt to use the stolen passport yet again.

Instead of jettisoning the Visa Waiver Program, the administration, the President himself, and some Members of Congress want to expand it to reward certain countries for being good allies. There are other ways to show our appreciation than by further widening a security gap, it seems to me. Doing away with the Visa Waiver Program need not hurt tourism, trade, and our international image. As a committed internationalist and a former State Department official myself—I was the Inspector General there before becoming the Inspector General at Homeland Security. It was I, inci-

dentally, and my staff who recommended that we increase the number of visa applicants who were interviewed. I have always believed that the State Department in general, and its consular bureau in particular, are seriously underfunded. If significantly more resources were provided to State, they could hire the additional consular officers needed to process applications from these 27 countries so that their travelers would not need to wait unduly long for a visa to visit the United States. And while we would lose, admittedly, our reciprocal right to visa waiver countries without a visa, that, it seems to me, is a rather small price to pay to close a big security gap.

I just want to mention, in my statement I talk also, as you know, about the Visa Security Officer Program, the importance to my mind that the deadline with regard to the Western Hemisphere Travel Initiative, with regard to American passports, as to land and sea, be implemented on the deadline that is in the law, and we can talk about that, I hope, during the course of the question-and-answer period.

But I just want to end by noting, as you did, the New York Times article this morning. If, in fact, the Secretary is considering either ending the Visa Waiver Program with regard to Britain entirely or applying it to British citizens of Pakistani descent—which seems to me is ethically questionable and would be politically difficult. So as between the two, if either is chosen, it seems to me likely that the administration would jettison Britain from the Visa Waiver Program.

If we are going to do that, if we are contemplating doing that with regard to our closest ally, then I question whether we should extend the Visa Waiver Program to countries like Estonia, for example.

Thank you very much, Madam Chairman.

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

Chairman FEINSTEIN. Thank you very much, Mr. Ervin. I appreciate it.

Mr. Zimmer?

**STATEMENT OF BRIAN ZIMMER, SENIOR ASSOCIATE, KELLY, ANDERSON & ASSOCIATES, AND FORMER SENIOR INVESTIGATOR, COMMITTEE ON THE JUDICIARY, HOUSE OF REPRESENTATIVES, WASHINGTON, D.C.**

Mr. ZIMMER. Chairman Feinstein, thank you for this opportunity to share my thoughts on strengthening the security of international travel documents.

If one thinks of homeland security measures to prevent attacks and subversion by foreign terrorists as a patchwork quilt, it is evident that many of the patches which were absent before 9/11 have been put in place. The important premise is now generally accepted that identity documents needs to be physically very secure, very counter-resistant, and issued to people only after a thorough adjudication and authentication of source documents. This was not true before 9/11.

Some important security patches are still missing, and others in place are only stop-gap measures and require more work. The miss-

ing "security patch" of greatest concern to me is the lack of substantial use of passport and identity card reading technology to authenticate documents at ports of entry. Another critical "security patch" that continues to be put on the back burner is the establishment of exit controls at every port of entry. The sophistication of our terrorist opponents requires that the Federal Government close these holes in the blanket of homeland security.

Much has been accomplished to interrupt terrorist travel, and worthwhile initiatives have been undertaken by the administration to improve the security of travel documents, many of which are the result of congressional mandates and some initially proposed by Senator Feinstein and Senator Kyl.

In the appendix to my written testimony, I have listed legislation since 2001 affecting travel and identity document security, and those of us familiar with the work of Senator Feinstein and Senator Kyl will recognize many of their initiatives.

As a former House Judiciary staff member, it is particularly satisfying to see so much of the legislative branch's vision for improved security becoming reality.

The adjudication for U.S. passports is highly dependent on the identity authentication prior to issuing driver's licenses, and so the REAL ID Act is included among the legislation in the appendix to my written testimony. It needs to be recognized as a critical element in securing international travel documents that we issue. Since some of the other witnesses have pointed out, as have the Senators, some of the absences of the administration, I would like to point out a few of the recent accomplishments they have completed.

It is my view that the implementation of Western Hemisphere Travel Initiative for air travel to and from the United States in January of this year went off very effectively, to many people's surprise, including my own. This success occurred because of the thorough public outreach by the Federal agencies involved, the post office, and DHS's coordinated planning with airports and airline carriers.

There has been a continued active outreach, and comprehensive planning for the next phase of WHTI at land ports of entry. DHS is undertaking a renovation of the border infrastructure to improve inspections and expedite travel, and also accommodate new readers for the PASS card and passport.

The continued expansion of the Immigration Advisory Program is an accomplishment of this administration, required by Congress but, nonetheless, largely moving at a faster pace than I would have envisioned 2 years ago. It stops people from getting on planes bound for the United States when their identity documents do not measure up and, more importantly, when close inspection identifies them as high-risk travelers with actual or potential terrorist affiliations. With reference to Great Britain, this seems to me to be one of the more obvious immediate solutions that could be imposed prior to determination that they have to be dropped entirely. An effort should be made to see what could be done with that as soon as possible.

There have been continued improvements at US–VISIT. This goes on behind the scenes, but there is an improving consolidation

of watchlist indicators which works and directly applies to travelers under the U.S. Visa Waiver Program, and I think it is extremely important work that is going on there. I applaud those who are completing it.

I think we have to acknowledge the administration has expanded use of terrorist watchlists to screen passenger manifest lists of international flights and has moved it from a largely unautomated process 6 years ago to one that is highly automated today in which information is quickly put into the filters that apply to manifests.

There has been—not as rigorous as some would like, but much more rigorous than occurred before—enforcement of requirements on countries participating the Visa Waiver Program. We have to feel that, notwithstanding it was slower than we might have liked, today the passports of Visa Waiver Program countries are far more robust, and most of them have an improved adjudication process before issuing them.

In conclusion, I think the Administration has met many of the mandates, but I think is struggling to meet the rest, and I thank you for this opportunity.

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

Chairman FEINSTEIN. Thank you very much, Mr. Zimmer, and let me thank all of you.

I would like to begin with Mr. Noble. And, Mr. Noble, I am going to ask you about ten quick questions. I want it for the transcript. If you can answer yes or no or briefly fill in, you may want to fill in in writing later.

What kind of information is available on the Interpol database?

Mr. NOBLE. The stolen or lost passport number, the issuing country, whether the passport was stolen blank or lost, and the date of reported theft or loss. So no personal, no privacy information.

Chairman FEINSTEIN. Thank you. How many passports are registered in the database?

Mr. NOBLE. We have over 6.7 million passports registered and over 14 million total stolen travel documents. And I might add, Chairman, since your last hearings—and we monitor your hearings—Norway, Japan, and Sweden are all now participating countries.

Chairman FEINSTEIN. Oh, good. That is excellent.

How many passports are from visa waiver countries?

Mr. NOBLE. From visa waiver countries, we have about 2.7 million.

Chairman FEINSTEIN. And how many countries now contribute their data?

Mr. NOBLE. 123 countries, and just to highlight, 5 years ago when we started, we had less than 12 countries and 3,000 documents, and now we have 123 countries and over 14 million documents.

Chairman FEINSTEIN. How does data get into the database?

Mr. NOBLE. The country that is the owner of the passport enters the data directly.

Chairman FEINSTEIN. So who owns the data?

Mr. NOBLE. The country that issues the passport. Only they can enter it, only they can modify it, only they can delete it.

Chairman FEINSTEIN. Can another country add, delete, or modify U.S. data in the Interpol database?

Mr. NOBLE. No.

Chairman FEINSTEIN. How fast is the search of the Interpol database?

Mr. NOBLE. Instant, 2 to 4 seconds.

Chairman FEINSTEIN. Is it expensive to connect border entry points to the database?

Mr. NOBLE. The image that we have here for you is Switzerland. Switzerland was able to connect 20,000 of its law enforcement officers to Interpol's system for about 100,000 euros. And up there on that screen, you see the hits that have occurred between December 2005 and April 2007. And highlighted in red for you, Chairman, is the visa waiver country hits.

Chairman FEINSTEIN. And we do not currently use this database?

Mr. NOBLE. The U.S. uses this database for investigative purposes and also has run samples to see whether or not it works. But on a real-time basis, when people are entering the country, the system is not yet being consulted regularly by the U.S. But as you heard and as I read in the newspaper, the plans are for it to occur by this fiscal year or at the latest this calendar year.

Chairman FEINSTEIN. I am very pleased to hear that. One last question. How much training is required to use the system?

Mr. NOBLE. The same training that is required to scan the passport for purposes of it being searched at the national level. Once the passport is scanned, a light flashes up, either green or red, indicating whether or not there has been a hit. So very easy.

Chairman FEINSTEIN. Well, let me just say to you, I really hope we get into this system in a robust way. I am very worried. This country is still like a sieve. You know, Mr. Zimmer mentioned the US–VISIT program. We still cannot tell if people who come into this country ever leave. And I do not think the American people understand how lax our controls really are.

I am going to follow up, and I am very grateful for you being here to see that we do get into this system. I think it is important.

Mr. NOBLE. Could I just follow up with one other point that you made?

Chairman FEINSTEIN. Yes, please. go ahead.

Mr. NOBLE. Because there have been some strong comments made about what should happen with regard to visa waiver countries. I do not want to get involved in a matter that does not concern me directly, but I would say that if the U.S. is thinking about eliminating the visa waiver for all of those countries that right now are some of your strongest partners in the fight against terrorism, I would try an interim response first. An interim response, I believe, is the same response that we use every day with our credit cards. If our credit card is lost or stolen, it takes us a matter of seconds or minutes for us to report that and even less time for the credit card company to cancel it.

If we were to require all countries to report theft of stolen blank passports, which you highlighted, which is a major problem, and if it was put into the system instantly, and if all countries were required to have the system to check it instantly, it would have no value to—

Chairman FEINSTEIN. What do we need to do that?

Mr. NOBLE. This is what the U.S.—I am sorry for pointing. This is where they were sitting before. Excuse me, sir. The U.S. is planning to do that, and I want to give you one case example to explain this.

On April 23, 2003, there was a theft of 850 passports in Cyprus, 850 blank passports, on April 23rd—

Chairman FEINSTEIN. Of this year.

Mr. NOBLE. 2003. 2003.

Chairman FEINSTEIN. OK.

Mr. NOBLE. On January 20th of this year, 11 Iraqis were stopped at Monterrey, Mexico, because an immigration officer asked one of them a question that made him suspicious. Eventually, it turned out that these 11 Iraqis had 8 of the passports that had been stolen way back in 2003. But for those immigration officers stopping the persons in Monterrey, their plans were to get to California and then claim asylum.

For us, we cannot take comfort by the view that there are a number of people, honest people, hard-working people, who want to claim asylum. We have to remember that the first World Trade Center attacks occurred by Ramzi Yousef carrying a stolen Iraqi passport and claiming asylum in order to get into the U.S.

These same passports, after Interpol got member countries together, turned up in March and April in Spain and in Poland, and from this one case were able to dig down and identify 14 people and identify a trafficking ring.

So it is one thing to connect to the system, but we also need to make sure that, as my colleague to the left said, that if and when there is a hit, we do not give them the passport back and we do not ignore that the hit has occurred.

Thank you.

Chairman FEINSTEIN. Thank you very much.

Just in response, I do not think the United States is preparing to do away with the Visa Waiver Program per se. I hope there is a greater recognition of the hazards it presents because we do not even know if these people go home.

Mr. NOBLE. Understood.

Chairman FEINSTEIN. I mean, once they come to this country, they are lost, effectively. And this is over 15 million people a year from 27 countries. This is a lot of people.

So if I might, Mr. Zimmer, you mentioned that you think progress is being made with the US–VISIT program, and I am delighted to hear that. Do you think there is much progress being made with respect to identifying when people are actually leaving the country who are here?

Mr. ZIMMER. No, I do not, and personally, a Congressman that I worked for—and, of course, I worked with your staff over the years—it remains a deep concern to me that people at the State level are so indifferent to this, because a majority of the States would have the same option of adding lost and stolen passports from Interpol. They would not have to go through the Federal Government. None of them are interested in this project that I know of, despite its wide publicity. And a majority of them will issue a driver's license, at least a temporary one, but many will issue one

for the full term based on any passport presented with no other identification. So it is a serious issue.

Chairman FEINSTEIN. Thank you.

Mr. Ervin?

Mr. ERVIN. May I add something to that, Chairman?

Chairman FEINSTEIN. Yes, you may.

Mr. ERVIN. As you know, surely, a few months ago, I think about 6 months ago or so, Secretary Chertoff or the Department, anyway, announced essentially that the Department had given up on the notion of having an exit feature to US–VISIT because of the cost. And it seems to me, as you said, that this is a huge vulnerability. If, in fact, it is subsequently learned that we have inadvertently admitted a terrorist in this country, as you say, we have no way of knowing whether that person definitively has left the country.

The US–VISIT system is incomplete and, to some degree, ineffectual, as long as it does not have a complementary exit feature.

Chairman FEINSTEIN. I would agree with that 100 percent.

Mr. Noble, over 420 million travelers come into the United States each year. This gives, I think, Americans the scope of this. So many people come here. Is the Interpol database equipped to handle that many inquiries?

Mr. NOBLE. Recognizing how careful you are about the record that is established here, I want to be very careful.

Interpol's system can handle triggering the fact that a passport that has been reported stolen or lost is being used. But then afterwards, there is a verification process that is required, where human beings have to determine whether or not the passport has been stolen, whether or not the passport has been lost. And for that volume of people, we are going to need human resources.

Right now, as Secretary General of Interpol, I do not have one human being from the Department of Homeland Security assigned to Interpol headquarters in Lyon. We do not—

Chairman FEINSTEIN. Is that right?

Mr. NOBLE. Not one. We have Secret Service—

Chairman FEINSTEIN. Homeland Security has—what?—over 200,000 employees. That is amazing.

Mr. NOBLE. To me it is amazing, and I am going to try to beg the Secretary tomorrow to change that.

The USNCB, which gets 10,000 messages per month, has vacancies. We believe we are a hub that can leverage the support that the U.S. gets around the world. But if the U.S. does not think it is important enough for Homeland Security to send people to work at Interpol, even though we developed these systems, even though we are the ones that invented it based on the U.S. feedback, it is hard for us to persuade other countries to dedicate the resources.

I think with all of the human beings they have working in the Department of Homeland Security, they could find a handful of human beings to send to the USNCB and to Interpol headquarters to work on this important issue.

Chairman FEINSTEIN. Well, I would agree, and I hope to see Secretary Chertoff this afternoon, and I will mention it to him, that is for sure.

Is it possible to screen people through Interpol before planes land in the U.S.? If so, how would that work?

Mr. NOBLE. When I used to be the Chairman of the Financial Action Task Force, we were working for the system of currency transaction reports and suspicious activity reports where banks are required to send to the U.S. Government any currency transactions above a certain amount.

In our view, if you required the same thing of airlines or airline reservation companies or of banks, you do not have them send personal data; you have them send to the U.S. Government the numbers of the passports being used for purposes of getting on an airline, making a reservation, or opening a bank account. Then a U.S. agency can get the information and actually decide whether or not the hit should lead to a disruption or actual monitoring and following of the individual.

So I believe that could be a very important legislative—

Chairman FEINSTEIN. I just asked my staff, isn't that being done now? And you are nodding yes. Perhaps could you just add to this.

Mr. BARTOLDUS. That is part of the AFIS transmission to the United States collected by CBP. The passport and the passport number is transmitted, and that will be what is used to bounce against the SLTD system by CBP.

Chairman FEINSTEIN. So, in other words, the manifest information comes before the plane leaves. Is that not correct?

Mr. BARTOLDUS. There is a rule out right now to change it from 15 minutes after departure to before the plane leaves. The final rule is about to be announced.

Chairman FEINSTEIN. OK. That is helpful. Would you let us know when the rule is announced?

Mr. BARTOLDUS. Yes.

Chairman FEINSTEIN. Thank you.

Mr. NOBLE. That is very helpful and very positive, but I am proposing that we could consider pushing it out even further before the person gets on the plane, before the person gets a ticket, to alert law enforcement in the country concerned that this person is, in fact, possessing a passport that has been reported lost or stolen. That would give the investigative agencies in the country where the person boards the opportunity to do something. It would give the law enforcement in the U.S. an opportunity to do something. And it would not involve any kind of privacy violations whatsoever for the individuals concerned.

Chairman FEINSTEIN. In other words, the passport number, when you make your reservation, would automatically be checked—we should look at that, too.

Mr. NOBLE. Yes, and then the hits would be sent out to the country that the airline will transit through, the end destination, and the origin of the passport. And that way, like with the Bank Secrecy Act, you can determine whether or not to investigate it overtly or investigate it covertly.

Chairman FEINSTEIN. Do other nation's airlines do this now?

Mr. NOBLE. No.

Chairman FEINSTEIN. No one does it now.

Mr. NOBLE. No one does it. No one does it. It is the first time it is being proposed, here today. And the goal is—I do not know how to think about this. Sometimes I think of borders of the U.S. as being the front-line defense, and sometimes I think of them as

being the last line of defense. And one of Interpol's goals is for countries around the world to view the effort as being a mutually important sharing of responsibility. So if we could get the airlines to send this information to Interpol's database—and we do not kick the information back to the airlines, so we do not tell them whether there is a hit or not. We just have it go to the law enforcement agencies, and they can make the determination about what to do. And we would have more than the time that it takes for the plane to take off and land in a country. I think it would be an extraordinary contribution to the problem of—

Chairman FEINSTEIN. I think it would, too, and it would certainly prevent mistakes being made on board, you know, by crew and pilots. So it might be very, very useful.

I think the time is moving on, but let me say thank you very much to the panel, and let me ask Mr. Ervin and Mr. Zimmer, do you have anything you would like to add at this point?

Mr. ERVIN. Well, there are a number of things, Senator, but if I could just make one point on this last issue.

Chairman FEINSTEIN. OK.

Mr. ERVIN. I do not have it in front of me, but I noted in my book last year that there was an offer made to Secretary Chertoff that I became aware of, and I think it was a September 2005 letter from the Air Transport Association, that lobbying organization, and the Association of European Airlines to make the passenger manifest available to the United States Government at the time of check-in—not an hour before, and certainly not 15 minutes after the flight leaves, but at the time of check-in. And we all know now in the post-9/11 world, the check-in happens probably 2 to 3 hours before the flight leaves.

Chairman FEINSTEIN. That is right.

Mr. ERVIN. To my understanding, the Department has yet to take these two key institutions up on that offer. Obviously, if the passport numbers were then checked at that time, that would be a tremendously useful tool.

Chairman FEINSTEIN. I agree with that. I think that is a very good idea, and we will write a letter to Secretary Chertoff with that in it.

Mr. Zimmer, any farewell comments?

Mr. ZIMMER. I will be brief. U.S. passports issued prior to the latest passport will remain in circulation and active use for border entry until 2016. Every major Mexican city near the border has a fairly substantial black market in lost and stolen passports and B–1 and B–2 crossing cards, which are often rented, by the way, by their legitimate owners. And, by the way, you could probably arrange for a clandestine visit and see one yourself if you are willing to disguise yourself. They are not at all secret and subtle, and these cities are easy to find. In fact, you just hold your hand up like this, and someone may walk up to you and take you there.

Chairman FEINSTEIN. Is that right?

Mr. ZIMMER. That is correct. Even though you would have to be a little bit less sophisticated in appearance than you are today.

But the reason I point that out is that these markets are open to all comers, whether you are Iraqi, Polish, Argentine. They are available. Americans buy documents there when they have issues

with their identities in the United States and can come back in with a valid passport containing a photo to which they have a close resemblance. This is the most difficult thing to detect at the border—an imposter who looks like the photo in the passport and who has memorized the details on the passport.

Much of that could be stopped by changes in the procedures of the border inspectors and by the introductions of machines. This has been resisted by CBP since long before 9/11, and the machines themselves have been out there for 4 or 5 years. They are used extensively throughout Scandinavia. They are rolling out across Europe where countries are becoming more aware of this. The technology is there. It is backed by software that lists thousands of documents and to which lost and stolen passport data could easily be added so that they could be read. It also determines whether they are counterfeit documents.

This is not that expensive, and it would absolutely stop most of this market in Mexico, and I understand it is growing in Canada, which makes sense.

So I think this is an unbelievably overlooked opportunity. All the legislation is there. It is not expensive, but it is going to take a change in culture and concept at Customs and Border Patrol.

Thank you.

Chairman FEINSTEIN. Thank you. I think that is a very helpful suggestion. We know the machines are there, but I am told the readers are not. They cannot read the machines, and so that is a problem.

Mr. ZIMMER. Excuse me, ma'am. Your legislation in 2002 required them to put 1,000 scanners, and they do work, and so far they are using less than 500 of them. They have been mostly sitting in warehouses.

Chairman FEINSTEIN. So you are saying they can read—

Mr. ZIMMER. Absolutely. They simply choose not to use the reading machines they already purchased, nor have they upgraded with the more sophisticated readers that are available and are regularly purchased by countries like Iceland and Sweden, which read, again, thousands of documents.

These have been demonstrated at some of the technology conferences. I think I was here at one 18 months ago on the Senate side where there was a choice of three of these machines from three different vendors. So you do not even have a sole-source issue.

Thank you.

Chairman FEINSTEIN. Thank you. Well, I think this has been very interesting, and I know Senator Kyl's staff is here, and I think we might do some joint letters and flesh out some of the things that have been developed here this morning and get more information and hopefully encourage some changes.

I would like to thank you very much for being here, especially you, Mr. Noble, for coming all the way across the Atlantic. We appreciate it very much.

Thank you, gentlemen, and the hearing is adjourned.

[Whereupon, at 11:55 a.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

# QUESTIONS AND ANSWERS

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Dianne Feinstein (#1)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

For those people applying for a U.S. visa, is the foreign passport checked against the U.S. databases on lost and stolen passports? If not, why not?

**Answer:**

All passports submitted for visa processing are checked against the CLASS database, which includes information on lost and stolen foreign passports, as part of an automated screening system.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Dianne Feinstein (#2)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

Does Consular Affairs have access to the FBI's "NCIC" – or criminal database – system? If so, are foreign passports checked against the NCIC database as a matter of routine? If not, why not?

**Answer:**

All FBI NCIC records on non-U.S. persons have been incorporated into CLASS and daily updates are received. All visa applications are checked against the database.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Dianne Feinstein (#3)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

Does Consular Affairs have access to the Interpol database on lost and stolen passports? If so, are foreign passports checked against the Interpol database as a matter of routine? If not, why not?

**Answer:**

The State Department currently obtains data on lost and stolen passports from a number of different sources, including directly from some foreign governments. The Bureau of Consular Affairs does not at present have direct access to Interpol's database. The Department of State, in coordination with the Department of Homeland Security, is working toward direct access to Interpol's Stolen and Lost Travel Document (SLTD) data as the hub of a multilateral system. Meanwhile, many countries submit lost and stolen passport data to both Interpol and the U.S. Government.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Charles Schumer (#1)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

1. Please provide the most precise current estimate of the date by which the Administration will make the proposed People Access Security Service (PASS) Card available to the public, or will make available another passport alternative that meets the requirements of Section 7209(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.

**Answer:**

The Department of State has developed an ambitious and aggressive schedule to develop the passport card. The Request for Procurement to industry was issued on May 25, and we expect to begin testing product samples in the summer. In accordance with testing requirements established in the certification by NIST, we will conduct the full range of security, durability, and privacy tests on the passport card and protective sleeve to ensure we are issuing the best and most secure card to the U.S. public. Absent any technical challenges that may arise as a result of testing, we expect to begin issuing passport cards to the public in spring 2008. The Departments of State and Homeland Security will conduct robust public outreach, particularly in border communities.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Charles Schumer (#2)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

2. What is the status and progress of the pilot project the State of Washington to develop and test drivers' licenses that would serve as travel documents for the purposes of the Western Hemisphere Travel Initiative (WHTI)?

**Answer:**

We understand that the Department of Homeland Security is working with the State of Washington on a pilot program for an "enhanced" drivers' license, which they intend to use as a possible model for other states. As the Department of State does not have an active role in this program, we respectfully refer this question to the Department of Homeland Security for appropriate response.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Charles Schumer (#3)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

3. By what date does the Department of Homeland Security expect to complete this pilot project with the State of Washington?

**Answer:**

We understand that the Department of Homeland Security is working with the State of Washington on a pilot program for an "enhanced" drivers' license which they intend to use as a possible model for other states. As the Department of State does not have an active role in this program, we respectfully refer this question to the Department of Homeland Security for appropriate response.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Charles Schumer (#4)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

4. What specific steps, if any, have the Department of State and the Department of Homeland Security taken to ensure that the database that will be used in conjunction with the PASS Cards or other passport alternative is secure from predation by identity thieves or terrorists?

**Answer:**

The information collected from American citizens for the passport card will be the same personal data collected for the passport book and will be collected and secured in the same manner as a regular passport application. The Department of State currently provides the Department of Homeland Security passport data held in the Passport Information Electronic Retrieval System (PIERS) through the Consular Consolidated Database (CCD) for use by the Customs and Border Protection Agency at U.S. ports of entry. The personal data for the passport card will be available for use by CBP in the same manner.

**Questions for the Record Submitted to**
**Director Andrew Simkin**
**Senator Charles Schumer (#5)**
**Subcommittee on Terrorism, Technology and Homeland Security**
**Committee on the Judiciary**
**May 2, 2007**

**Question:**

5. What specific steps, if any, have the Department of State and the Department of Homeland Security taken to ensure that, following implementation of WHTI, U.S. travelers who do not have WHTI-compliant documents will nevertheless be able to cross the border on an emergency or expedited basis for special circumstances, such as a funeral?

**Answer:**

Procedures and documentary requirements at port of entry fall under the jurisdiction of the Department of Homeland Security's Customs and Border Protection, which currently has procedures in place at ports of entry to process improperly documented American citizens. Although we and DHS have not yet determined what additional procedures will need to be established to facilitate emergency travel to WHTI countries, we continue to address this in our discussions with a view toward resolution before final implementation. We are also aware of the concerns of emergency responders and are addressing them to prevent any interruption in emergency services.

**Answers from Paul Morris and Michael Everitt to Senators Schumer and Senator Feinstein**

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | PASS |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Charles E. Schumer |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Please provide the most precise current estimate of the date by which the Administration will make the proposed People Access Security Service (PASS) Card available to the public, or will make available another passport alternative that meets the requirements of Section 7209(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.

**Answer:**
The Department of State (DOS) has developed an ambitious and aggressive schedule to develop the Passport Card. The Request for Procurement (RFP) to industry has been issued, and DOS expects to begin testing product samples this summer. In accordance with testing requirements established in the certification by the National Institute of Standards and Technology (NIST), DOS will conduct the full range of security, durability, and privacy tests on the Passport Card and protective sleeve to ensure we are issuing the best and most secure card to the American public.

Absent any technical challenges that may arise as a result of testing, we expect to begin issuing the cards to the public in Spring 2008. DOS and the Department of Homeland Security (DHS) will conduct a robust public outreach program for those border communities where DHS is installing the RFID vicinity infrastructure. The focus will be the high volume land ports of entry across both the northern and southern borders. The goals are to document Americans so that they can comply with the new requirement and to facilitate travel, trade, and tourism.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | pilot project |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Charles E. Schumer |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** What is the status and progress of the pilot project in the State of Washington to develop and test drivers' licenses that would serve as travel documents for the purposes of the Western Hemisphere Travel Initiative (WHTI)?

**Answer:**
The Washington State Memorandum of Agreement (MOA) was signed on March 23, 2007, between the Secretary of Homeland Security and the Governor of the State of Washington. The MOA established the foundation to develop, test, issue, and evaluate an enhanced state-issued driver's license that could be used as an acceptable document for WHTI at land and sea ports of entry. The DHS - Washington State working group is now in the process of finalizing functional and technical requirements.

**Question:** By what date does the Department of Homeland Security expect to complete this pilot project with the State of Washington?

**Answer:**
Absent any technical or operational challenges that may arise, it is anticipated that Washington State will begin issuing enhanced driver's licenses by January 2008. DHS will periodically evaluate the success of this program and make a determination about its continuation at the appropriate time.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | PASS cards |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Charles E. Schumer |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** What specific steps, if any, have the Department of State and the Department of Homeland Security taken to ensure that the database that will be used in conjunction with the PASS Cards or other passport alternative is secure from predation by identity thieves or terrorists?

**Answer:**
Passport data provided to U.S. Customs and Border Protection (CBP) by the Department of State is protected in accordance with all applicable laws. Information Security requirements as specified in CBP Handbook (HB) 1400-05C, and the DHS 4300A Sensitive Systems Handbook, as well as applicable NIST guidance, are applied to sensitive data such as passport data. In addition to information security best practices, all personnel, including CBP Officers making inquiries into the database, have had a full field background investigation and are given information on a "need-to-know" basis only. Procedural safeguards are in place to include accountability, receipt records and audit trails. Additionally, the facility that houses these databases has physical security that includes restricted access with alarm protection systems, special communications security, and security fencing with armed guards patrolling the area.

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | special circumstances |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Charles E. Schumer |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** What specific steps, if any, have the Department of State and the Department of Homeland Security taken to ensure that, following implementation of WHTI, U.S. travelers who do not have WHTI-compliant documents will nevertheless be able to cross the border on an emergency or expedited basis for special circumstances, such as a funeral?

**Answer:**
Although WHTI imposes passport requirements or other approved entry documents for travel into the United States, WHTI also provides for situations in which documentation requirements may be waived or persons paroled into the country on a case-by-case basis for unforeseen emergencies or for humanitarian or national interest reasons, such as first responder action, response to natural disasters, patients or family members involved in medical emergencies, etc.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | fraudulent passports |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**

According to a May 6, 2007, Washington Post article, "U.S. to Use Interpol Passport Database for Screening," an unnamed U.S. Department of Homeland Security official reported that "in a test of 1.9 million passport records collected over 16 days by US border officials in April, DHS personnel discovered 273 stolen documents using the Interpol data. Analysts cleared 219 cases, but 64 remained unresolved." (These were the original numbers provided to CBP.

If a case cannot be cleared, what happens to the traveler? Is the traveler admitted into the U.S.?

**Answer:**

In conjunction with CBP's National Targeting Center, the port of entry can perform queries in a variety of systems (Treasury Enforcement Communications System - TECS; Consular Consolidated Database - CCD; and United States Visitor Immigrant Status Indicator Technology - US-VISIT) that include biographic and biometric information in order to determine whether a passenger is the true bearer of the document presented. If a passenger is determined to be the true bearer of the travel document and no other violations are discovered, the passenger is admitted into the United States.

The Washington Post referred to a test pilot project conducted April – June 2006 where Interpol U.S. National Central Bureau (USNCB) and CBP compared Advance Passenger Information System (APIS) passport information to the Interpol Stolen and Lost Travel Document (SLTD) database in order to make an estimate of the resources required for real-time query capabilities by border officials at the ports of entry (POEs) to the SLTD.

The comparison between the APIS data and the SLTD was for an exact match to both document number and country of issuance. Of the discovered matches, 64 could not be verified as having been presented by the true bearer of the document. These documents were forwarded to member country National Central Bureaus (NCBs) for confirmation of document status.

Out of the 64 requests sent to foreign NCBs, only 14 responded. The USNCB indicates that in these cases the passport in question was reported as lost or stolen but subsequently recovered by the true bearer of the document. The true bearer then utilized the reported travel document for travel. Of the replies received, it has taken foreign NCBs an average of 15 1/2 days to respond to a request. The shortest time was 14 days and the longest time was 17 days.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | fraudulent passports |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**

Were the holders of fraudulent passports arrested?

**Answer:**

This was a test project conducted post-travel and meant to make an estimate of the resources required for real-time query capabilities by border officials at the ports of entry (POEs) to the SLTD. To date, USNCB and CBP analysis have not confirmed the misuse of any of the documents that matched the Interpol Stolen and Lost Travel Document database, and none was used to fraudulently enter the United States. However, CBP did refer 3 cases to Immigration and Customs Enforcement (ICE) for further investigation. No determination has been made as to the validity of the documents.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | passenger data |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**

What plans, if any, does the United States government have for checking passport data against Interpol databases before the passenger boards the plane bound for the U.S.? How would these plans apply to passengers from Visa Waiver Program countries?

**Answer:**
CBP published the Pre-Departure Notice of Proposed Rulemaking (NPRM) in the Federal Register on July 14, 2006, and under the proposed rule carriers would be required to submit an electronic manifest prior to departure. The NPRM also provided for a transmission option called APIS Quick Query (AQQ), which would allow carriers to provide passenger data at the time of check-in.

CBP currently screens passengers no later than 15 minutes after departure per the Advance Passenger Information System (APIS) Final Rule (AFR), which was published in the Federal Register on April 7, 2005.

CBP will screen passengers against the Interpol SLTD in conjunction with current procedures to screen passengers against the 3,434,948 records of Lost and Stolen Travel Documents that have been incorporated into CBP systems. This screening process will occur while the passenger is airborne.

In an effort to extend our zone of security outward, the Immigration Advisory Program (IAP) posts CBP officers overseas at high-volume, high-risk airports to screen passengers before they board aircraft destined for the United States. The IAP has two major objectives: to enhance the security of air travel by preventing terrorists from boarding commercial aircraft destined for the United States, and to reduce the number of improperly documented passengers traveling from or through a country to the United States.

In addition to a layered defense strategy that includes lookouts on fraudulent passports, CBP officers are trained to identify travelers utilizing in a fraudulent manner stolen or lost travel documents belonging to victims of theft or those who have simply misplaced their passports. CBP does not rely solely on the lookouts as the single source for identification of mala fide travelers. CBP also conducts interviews of suspected mala fide travelers and utilizes fraudulent document detection techniques.
The same procedures are used on travelers from process screening travelers from Visa Waiver Program (VWP) countriesAir carrier data is processed and matched against Interpol watch lists based on the APIS data provided. The CBP screening process does

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | passenger data |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

not differentiate between country of citizenship. Citizenship becomes a factor in determining admissibility when a passenger presents himself/herself for admission to the United States.

**Question:**

At what point does the U.S. government obtain the passenger manifest of flights bound for the United States?

**Answer:**

The APIS Final Rule (AFR), published in the Federal Register on April 7, 2005, requires commercial air carriers to submit an electronic manifest no later than 15 minutes after departure ("wheels up" on the aircraft) for United States-bound flights.

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | Offer |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**
Secretary General Noble noted in his testimony that there was an offer made in September 2005 from the Air Transport Association and the Association of European Airlines to make the passenger manifest available at the time of check-in. Has the Department taken these two institutions up on that offer? If not, why not?

**Answer:**
We are not aware of a formal offer. However, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 required the U.S. Government, where practicable, to conduct terrorist watch list screening prior to a traveler's departure. CBP published the Pre-Departure Notice of Proposed Rulemaking (NPRM) in the Federal Register on July 14, 2006, and, under the proposed rule, carriers would be required to submit an electronic manifest prior to departure. The NPRM also provided for a transmission option called APIS Quick Query (AQQ), which would allow carriers to provide passenger data at the time of check-in.

Under current regulations carriers are required to submit an electronic manifest no later than 15 minutes after departure for flights arriving into the United States. However, carriers can submit data earlier, including at the time of check-in. In the air environment, manifest data is normally transmitted 15 minutes after departure for arrivals into the US and 15 minutes prior to departure for departures from the US. Sea manifests are often transmitted several days in advance.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Interpol |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Does the Department of Homeland Security intend to assign personnel to the Interpol Headquarters in Lyon as the U.S. moves toward further cooperation with Interpol? If so, when? If not, why not?

**Answer:**
Interpol Secretary General Noble has requested that DHS consider detailing staff to Interpol Headquarters in Lyon, France. DHS is currently evaluating the benefits of this proposal to determine whether the significant costs incurred would add sufficient value beyond the 9-12 DHS detailees already assigned to Interpol's Washington, D.C. office.

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | card readers |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**
I am concerned by the testimony of Brian Zimmer that "the missing security patch of greatest concern" is the "lack of substantial use of passport and identity card-reading technology to authenticate documents at ports of entry." The installation of the Biometric Verification System (BVS) was first mandated in Section 104 of Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

Is Customs and Border Protection (CBP) using the BVS card reader at all ports of entry? If not, how does CBP verify the identity of a person holding the BVS card?

**Answer:**

The BVS system is no longer used at ports of entry. DHS has deployed the United States Visitor and Immigrant Status Technology (US-VISIT) system, which provides the capability to perform biometric identity verifications on U.S. travel documents issued to foreign nationals. The Department of State provides digital Border Crossing Card (BCC) data to the US-VISIT Automated Biometric Identification System (IDENT). With this information available, CBP officers are able to perform a biometric verification for the traveler requesting admission. The system captures the traveler's fingerprints and compares them to the fingerprints submitted at the time of BCC issuance. BCC biometric verification is now performed as an integrated part of the US-VISIT process when travelers apply for an I-94 to enter beyond the border zone (25 miles or 75 miles in Arizona) or stay longer than 30 days.

In addition to the US-VISIT process, biometric verification is available for any traveler who had submitted biometrics to DHS at the time of their travel document application. Through the Secondary Inspection Tool (SIT) which is available in secondary at all ports of entry, CBP officers can perform a biometric identity verification. The SIT provides a one to one comparison between a live capture of biometrics to the biometrics on file for the travel document. In the land environment, CBP officers can use the SIT to verify the identity of a person holding a BCC card when an I-94 is not being requested.

Additionally, CBP implemented a new primary inspection system that has been deployed at all pedestrian primary lanes. The system displays for the CBP pedestrian primary officer the BCC photograph that was taken at the time the BCC was issued. The photograph displayed to the officer must match exactly to that which is printed on the BCC card. The system provides for immediate fraud detection based upon any tampering with the photograph.

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | card readers |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Has CPB integrated the BVS card readers into the TECH/ IBIS system so cards can be verified more quickly? If not, why not? Has there been an analysis of such integration, including cost estimates? If so, when was this completed?

**Answer:**
The BVS readers presented numerous challenges for integration into the TECS system. Besides being a proprietary technology, the readers were found to perform poorly when there was any surface damage on the BCC itself. With the implementation of US-VISIT, biometric verification of the BCC became available with the technology and hardware used across all ports of entry.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | spot checks |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** When imposters are detected using the BVS readers, what action is taken against the imposters? Please provide a list of all imposters charged with attempting to cross the border with a (1) valid B1/B2 card that was not issued to them, (2) counterfeit or altered B1/B2 card.

**Answer:**
Imposters intercepted at ports of entry are inadmissible to the United States pursuant to section 212(a)(6)(C) of the Immigration and Nationality Act (INA). In general, arriving aliens who are inadmissible under section 212(a)(6)(C) and/or 212(a)(7) of the INA are subject to expedited removal pursuant to section 235(b)(1). In addition to determining the validity of each document presented for inspection, CBP officers must examine the document to determine whether it has been altered through data eradication, photo substitution, page substitution, or counterfeiting. CBP officers also must compare the photograph to the person presenting their entry document(s) so as to ensure that the person is not an imposter. Careful questioning of an applicant regarding the nature of his/her visit and the particulars of how the visa was obtained, as well as close scrutiny of the photo and biographic data on the travel document, assist officers in determining whether the bearer is the rightful holder of the passport or visa. CBP officers have been delegated authority, pursuant to 22 CFR 41.122(h), to cancel genuinely issued visas which are presented by other than the rightful holder.

For privacy and law enforcement reasons we cannot provide a list of persons intercepted, but can provide general statistics on the number of imposters using BCCs and the number of counterfeit and altered BCCs intercepted.

| | Impostors | Counterfeit/Altered |
|---|---|---|
| Fiscal Year 2006 | 16,181 | 647 |
| Fiscal year 2007 to April | 8,556 | 549 |

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | spot checks |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**
Has CBP placed card readers at primary inspection points that would allow "spot checks" without referring travelers to secondary with the attendant extra time and delay? If not, why not?

**Answer:**
For the BVS system, each location received as many BVS readers as could reasonably fit in the facility (e.g., 33 were deployed to San Ysidro). CBP officers used the BVS devices to verify the biometric of the person presenting the card to the biometric encoded on the card. This process was performed in the secondary inspection area for those individuals referred from vehicle and pedestrian primary inspection lanes due to a variety of reasons, including "hits" on CBP enforcement systems or suspicions raised during the primary inspection process. If further inspection was necessary, the officers had the option to conduct the BVS process at primary or refer to secondary depending on the pedestrian traffic volume. This has now been replaced with the US-VISIT biometric verification process available at all ports of entry.

CBP has implemented a new pedestrian primary inspection system that displays for the CBP primary officer the BCC photograph that was taken at the time the BCC was issued. The photograph displayed to the officer must match exactly to that which is printed on the BCC card. The system provides for immediate fraud detection based upon any tampering with the photograph for all travelers processing through a pedestrian primary inspection with a BCC or any other U.S.-issued travel document.

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | unused card readers |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**
Are there card readers that are simply not being used and are, as Mr. Zimmer suggested, simply being held in warehouses? If so, why?

**Answer:**
We are unaware of any "unused" readers in a warehouse. Customs and Border Protection (CBP) deployed readers as an interim measure, but no longer needs them due to advances in technology and database migration. The BVS readers only read BCC and License Plate Reader cards, and the technology was proprietary. These were deployed by CBP to the land border POEs as an interim solution to perform biometric verification until a centralized biometric verification solution was developed. BVS was used in a stand-alone mode that took additional inspection time and did not check whether a card was still valid or conduct any biometric watchlist checks. These deficiencies have now been addressed with the availability of the digital BCC data provided by the Department of State, including the full database of BCC fingerprints within the US-VISIT IDENT biometric database. With this availability, BCC verification is now performed as an integrated part of the US-VISIT process, including name and date of birth checks against DHS and FBI watchlist databases, fingerprint checks against the IDENT database for both watchlist and 1:1 verification checks, and document validation checks, which provide issuance information and tell whether a card has been revoked since its issuance.

| | |
|---|---|
| **Question#:** | 14 |
| **Topic:** | document verification |
| **Hearing:** | Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:**
Since the pilot, has CBP ever run 100% document verification at any of the Southern border points of entry? If so, which ports, on which days? Were the BVS readers deployed to conduct 100% verification of B1/B2 cards during those document verification exercises? What were the results?

**Answer:**

CBP performs visual inspections on all travelers requesting admission into the United States. Additionally, those travelers requiring a document to enter the United States undergo document inspections. The BVS system was an interim step to verify the biometric data of a person presenting a card to the biometric data encoded on the card. The BVS process was performed in the secondary inspection area for those individuals referred from vehicle and pedestrian primary inspections lanes due to a variety of reasons, including "hits" on CBP enforcement systems or suspicions raised during the primary inspection process. The pedestrian primary inspection system displays the U.S.-issued travel document photograph that was taken at the time of document issuance for the CBP primary inspection officer. This capability provides for immediate fraud detection when a photograph has been tampered with, since the photograph displayed should match exactly to that which is printed on the U.S.-issued travel document. When further inspection is necessary, the officers can refer a traveler to secondary for biometric verification utilizing the US-VISIT system.

# SUBMISSIONS FOR THE RECORD

Statement of
Patrick D. Donovan
Assistant Director for Diplomatic Security
Director of Domestic Operations
Bureau of Diplomatic Security

Senate Committee on the Judiciary

Hearing on Interrupting Terrorist Travel:
Strengthening the Security of International Travel Documents

Room 226 Dirksen Senate Office Building
May 2, 2007
10:00 a.m.

Good morning Chairwoman Feinstein, Ranking Member Kyl, distinguished Members of the Subcommittee;

I am honored to appear before you today with my distinguished colleagues. I'd like to thank you and the Committee Members for your continued support and interest in the Bureau of Diplomatic Security's (DS) protective and investigative programs. Through Congressional support, DS safeguards American diplomats and facilities around the world and protects the integrity of U.S. travel documents. With your permission, I would like to present a brief statement and submit a copy of our Visa and Passport Security Strategic Plan as my full testimony for the record.

One of the most critical national security challenges that the American will face for the foreseeable future is the desire by terrorist groups and individuals to inflict catastrophic harm to the United States. A key element in all terrorist operational planning is access to their target. Such access requires the acquisition of travel documents (including visas and passports) that allow terrorists to enter, and move freely within, our country.

As the law enforcement arm of the Department of State, DS is responsible for upholding the integrity of the U.S. visa and passport through enforcement of relevant portions of the U.S. Criminal Code. DS is the most geographically extensive federal law enforcement agency in the United States Government, with approximately 1,400 Special Agents dispersed among 25 field and resident offices domestically, with representation on 26 Joint Terrorism Task Forces, and with assignments to U.S. embassies and consulates in 159 countries. DS is uniquely positioned and committed to meet the serious national security challenge of travel document fraud. Our agents conduct investigations into passport and visa fraud violations wherever they occur. Our partnership with the Bureau of Consular Affairs has enabled us to jointly focus on protecting the U.S. passports and visas.

Overseas, we work with foreign partner nations to target and disrupt document fraud rings and human smuggling networks. Domestically, we work with local, state, and federal law enforcement agencies to investigate, arrest, and seek prosecution of fraud violators. Throughout this global network of law enforcement professionals, DS Special Agents are on the frontlines of combating terrorist and criminal travel.

Terrorists targeting the U.S. attempt to discover, manipulate, and exploit vulnerabilities within our travel document system. To successfully counter this threat, DS has crafted a Visa and Passport Security Strategic Plan that leverages our international expertise and worldwide presence. The Plan provides the framework for a worldwide Visa and Passport Security Program and will significantly augment the Department's ongoing efforts to prevent terrorist travel. Our approach incorporates the principles of the National Strategy to Combat Terrorist Travel and addresses the objectives of the Intelligence Reform and Terrorism Prevention Act of 2004.

The Strategic Plan requires the deployment of additional DS personnel to critical posts worldwide, resources to enhance our intelligence and data-sharing efforts, and training and technical assistance to our foreign partners. Presently DS has Special Agents assigned to consular sections abroad to focus solely on travel document fraud. By the end of this year, DS will have 33 Special Agents assigned to key posts investigating travel document fraud. By the end of 2008, DS will have 50 agents in such capacity. Since 2004, the results have been promising, yielding nearly 1,050 arrests for document fraud and related offenses; in excess of 3,400 visa refusals and revocations; and more than 6,200 foreign law enforcement and security personnel trained.

The Plan is built upon a cornerstone of three strategic goals:

- To defend the U.S. and our foreign partners from terrorist attack through aggressive, coordinated international law enforcement actions and initiatives;
- To detect terrorist activity, methods of operation, and trends that exploit international travel vulnerabilities; and
- To disrupt terrorist efforts to use fraudulent travel documents through strengthening the capabilities of our foreign partners by such highly successful programs as the DS Anti-Terrorism Assistance Program.

Our Strategic Plan offers a comprehensive and proactive approach to ensuring the integrity and security of U.S. visas and passports.

Thank you for the opportunity to brief you on this vital aspect of DS's mission. We look forward to your continued support.

**STATEMENT FOR THE RECORD OF CLARK KENT ERVIN, FORMER INSPECTOR GENERAL OF THE U.S. DEPARTMENT OF HOMELAND SECURITY BEFORE THE SENATE JUDICIARY SUBCOMMITEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY ON "STRENGTHENING THE SECURITY OF INTERNATIONAL TRAVEL DOCUMENTS" - MAY 2, 2007**

Thank you very much, Chairman Feinstein, Ranking Member Kyl, and other members, for inviting me today to testify before the subcommittee on the critically important topic of Strengthening the Security of International Travel Documents." This is **not** an academic issue. For whatever reason, all 19 of the 9/11 hijackers entered the United States through official ports of entry and, in so doing, used travel documents – visa and passports – to do so. Even though it is almost as easy today as it was then to enter our country illegally, without any travel documents at all, it is certainly possible that terrorists in the future will likewise attempt to enter the United States through legal channels, attempting to exploit remaining vulnerabilities in travel documents to do so.

To be sure, and to be fair to the Administration, there certainly have been improvements with regard to travel documents, and related processes, in the last six years. The Departments of State and Homeland Security, in particular, are to be applauded for this. But, since my time is limited, and since I know that State and DHS will, quite understandably, highlight their respective achievements in this regard, I will focus my remarks on where security gaps remain and how, in my judgment, they should be closed.

*The Visa Waiver Program Should be Terminated*

To my mind, the greatest single vulnerability that remains lies in the visa waiver program. Terrorists put a premium on passports from the 27 countries whose citizens do not need visas to visit the United States, provided they intend to do so for a limited time (90 days) and for limited purposes (tourism or business). It is not for nothing that would-be shoe bomber, Richard Reid, was a British citizen, or that the man some think might have been the 20th 9/11 hijacker, Zacarias Moussaoui, was a French citizen. As my staff and I put it in a report we issued during my time as DHS Inspector General, "The visa is more than a mere stamp in a passport. It is the end result of a rigorous screening process the bearer must undergo before travel. By the end of the process, U.S. authorities have collected and stored considerable information about the traveler and the traveler's planned journey. When the visa is waived for broad classes of travelers, those travelers avoid this extensive examination and the United States does not collect comparable information regarding them."

In the post 9/11 world, most visa applicants (about 90% according to some estimates I have seen) are interviewed by U.S. consular officials at our embassies and consulates abroad. Many, if not most, of the interviewers are conversant in the language of the applicants, familiar with their customs, and trained in fraud detection techniques. Consular officials have the further luxury of spacing the interviews so as to maximize the time that they have to question applicants.

By way of contrast, there's no time for port of entry inspectors to interview visa waiver travelers. Hundreds of passengers disembark at any one time from international flights and inspectors feel pressure to clear them within forty-five minutes. And, even if they did interview passengers, most inspectors speak either only English. The relative few who speak another language speak Spanish, not languages like Arabic, Farsi, or Urdu spoken in "countries of concern."

Far more information is known about those traveling on visas, increasing the likelihood that the traveler is, in fact, who he says he is and that he is not a terrorist or connected to terrorism.

All visa applicants must complete a forty question form. Male applicants between the ages of sixteen and forty-five must complete a supplemental form. Applicants' name, birth date, place of birth, employment history, travel purpose and itinerary, visa history, and the immigration status of close family are obtained. Consular officials take prints of two of the applicants' fingers. This information is then stored in the Consular Consolidated Database, and much of it can be accessed electronically by port of entry inspectors to enable them to verify travelers' identities. The finger scans taken by consular officials abroad can be compared to the finger scans taken at the port of entry through the U.S. VISIT automated entry system to confirm that the person standing before the inspector is the very same person who applied for a visa.

The visa waiver traveler, on the other hand, gives only his name, present citizenship, country of residence, passport number, and address in the United States where he will be staying. While finger scans are taken at the port of entry, there is nothing to compare them to to confirm identity.

I pointed out in my book, *Open Target: Where America is Vulnerable to Attack*, last year that, at least as of then (and I have seen nothing to indicate that circumstances have changed since), it was relatively easy to obtain citizenship in certain visa waiver countries. At least as of then, only three years of residence were required to become citizens of Belgium, Sweden, and Denmark, respectively. Italian or Irish citizenship could be obtained "derivatively" and "virtually," without ever setting foot in those countries, by simply having a parent or grandparent with such citizenship.

But, terrorists needn't be born in a visa waiver country or subsequently acquire citizenship in one to get a passport from a visa waiver country. They can simply steal blank passports from government issuing offices and substitute their own photographs and biographical data for those of the real applicants, or they can steal already issued passports from unsuspecting holders.

During my time as DHS Inspector General, we investigated the problem of lost and stolen passports. Because of the laxity in reporting, we could not definitively determine the scope of the problem. But, we were able to get some sense of its magnitude, noting that 28 foreign governments reported that 56,943 of their passports were stolen between

January 2002 and January 2004. Intrigued by that number, we decided to focus on the nearly 4,000 blank passports stolen from visa waiver countries that were reported to the U.S. government from 1998 to 2003.

We found 176 attempts to use some of those passports to enter the United States. Some attempted entries were made before "lookout" notices were posted in Customs inspectors' computer systems indicating that the passports in question were stolen, and some were made after the lookout notices were posted. Aliens presenting stolen passports before lookout notices were posted for them were successful in being admitted to the United States 81% of the time. Shockingly, the success rate of aliens presenting stolen passports *after* lookout notices were posted was almost as high – 73%. Of the 57 aliens in the latter category, 33 were admitted into the country *after* 9/11, when, presumably, our border inspectors should have been on high alert. Even more incredibly, some of the aliens used stolen passports to enter the United States *multiple* times after lookout notices were posted. Because the then nascent U.S. VISIT system lacked an exit feature, there was no way to tell for sure whether any of those aliens had left the country. And, in any event, there was no formalized procedure to ensure that any such aliens were brought to the attention of the Department of Homeland Security's "ICE" (Immigration and Customs Enforcement) investigators so that the aliens could be tracked down and either prosecuted by us or deported to their home countries. At least some of the stolen passports at issue were linked in one way or another to 9/11, and yet ICE had not made a priority of investigating those cases. Finally, another shocking finding was that, in those instances where Customs inspectors rightly refused to admit people presenting passports known to be stolen, inspectors would sometimes allow the alien to return to his country of origin with the stolen passport. Of course, the alien should have been either prosecuted by the U.S. government and/or deported and the passport confiscated to prevent re-use. DHS duly promised to implement the recommendations that we made in our December 2004 report to address the lost and stolen passport problem, and otherwise to tighten the visa waiver program, but my long history with the department inclined me to be skeptical of that claim.

My skepticism proved to be warranted when the Government Accountability Office released its report to this very subcommittee last fall titled, "Border Security – Stronger Actions Needed to Assess and Mitigate the Risks of Visa Waiver Program." According to GAO, some visa waiver countries sometimes fail to notify our government when their passports are discovered to be lost or stolen. (One country waited *nine* years before advising Washington of the theft of nearly 300 of its blank passports.) Though countries have been required by law to do since 2002, as of last fall, DHS had yet to develop standard operating procedures for them to report passport thefts, including the means of reporting and the U.S. government entity to which such information should be reported. While most visa waiver countries contribute to Interpol's database, four do not, and even some of those countries that do report lost and stolen passport information to Interpol fail to do so occasionally. Furthermore, the Interpol database is not automatically accessible to U.S. border inspectors at primary inspection. To quote the report, "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 systematic access to Interpol's data." The problem continues to be a real one, not merely a theoretical vulnerability. From January to June 2005, DHS confiscated 298 visa waiver country passports that travelers were trying to use to enter the United States. Of course we do not know how many lost or stolen passports, if any, DHS failed to catch, or how many, if any, border inspectors spotted, but nevertheless permitted travelers to use to gain entry.

Another troubling development since our report in 2004 on this subject is DHS' decision a few months ago to give up on its goal of developing an exit feature to U.S VISIT. As a practical matter this means that if the department subsequently discovers that a known or suspected foreign terrorist was somehow admitted to the country at a legal point of entry at some point (on a lost or stolen passport or otherwise), there is no way to know for sure whether, and, if so, when that terrorist left the country.

Though, for the foregoing reasons, the visa waiver program remains a security gap (to say nothing of the laxity in DHS' review of countries' eligibility to continue in the program), the Administration and some in Congress want to expand the program to still more countries. This would be a serious mistake. As we put it in a report issued by the DHS Office of Inspector General in April 2004, "Every time a new country entered the VWP [Visa Waiver Program], its passports became valuable targets for counterfeiters, petty crooks who attempt photo substitutions, and organized criminals who steal blank passports, as well as forgers who use modern technology to create false identities in blank passports and criminal rings who manufacture phony identity documents in order to obtain VWP passports."

Rather than expanding the visa waiver program, we should end it. In the post 9/11 era, participation in the visa waiver program should not be held out as a carrot to entice other countries to support American policies. There are many other carrots at our disposal and many other ways of showing our appreciation that do not endanger our security.

I fully recognize that my position on this matter is controversial. I do not take this position lightly. I fully understand the benefits that it provides to our country. It serves to encourage foreigners to visit the United States, a time when I think it is more critical than ever before in our history that we be, and be seen as, a nation that is eager embrace the world. It enables our citizens to travel to these countries without our obtaining a visa from them. I travel abroad fairly regularly, and mostly to visa waiver countries. So, if enacted, my policy proposal could inconvenience me. But, the inconvenience of paying a fee and waiting some period of time to obtain a visa to visit a foreign country is, it seems to me, a small price to pay to close a gaping hole in our nation's security. And, of course, there need not be much inconvenience. If the State Department's budget were adequately increased, it could hire the requisite number of additional consular officers to ensure no material delay in the issuance of visas to a significantly greater number of applicants. As a committed internationalist, and the former Inspector General of the State Department as well as the Department of Homeland Security, I have long believed that the State Department has been shortchanged, particularly in the consular area.

*The Visa Security Officer Program Should be Expanded and Strengthened*

Another undertaking that could have the effect of enhancing the security of the visa process is expanding and strengthening the Visa Security Officer (VSO) program. The law creating DHS, the Homeland Security Act of 2002, established the program in Saudi Arabia and contemplated that it would ultimately be in place in virtually every embassy and consulate abroad from which visas to visit the United States are issued. VSOs were to be DHS personnel thoroughly familiar with visas, passports and other travel documents, trained in fraud detection, and cognizant of foreign countries and cultures and U.S. State Department protocol and procedures. They were to work side by side with State consular officers to provide a final check before issuance that visas are not inadvertently issued to terrorists. The rationale was that, as DHS personnel, VSOs would be naturally inclined to make security, rather than diplomacy and "customer service" a priority in the visa issuance process.

When we examined the then nascent program in Saudi Arabia in 2004 during my time as DHS Inspector General, we found that the program was not meeting its potential. At the time, there were no designated VSO slots; the positions were filled by volunteers. And, the volunteers were serving on only a temporary basis, resulting in a rapid turnover of personnel. The temporary volunteers were lacking in the basic skills needed to be effective. For example, one officer had no law enforcement experience. Another had never worked outside the United States, and, as a result, had no idea of how an embassy works. Another had no knowledge of the visa process. Only one of the 10 could speak Arabic. Even though the DHS VSOs and the State Department consular officers were located just a few feet from each other, neither could access the others' databases, so both were inputting and then sending back to Washington for a background check essentially the same information. As a consequence, precious time was being wasted by the State Department, the Department of Homeland Security, their respective headquarters, and other key members of the U.S. law enforcement and intelligence communities, leaving the VSOs little time to do what they were supposedly uniquely competent to do – reviewing visa applications from a strictly counterterrorism perspective.

The last review of the program that I am aware of is a GAO review about a year and a half ago, in September 2005. As of then, things were improving somewhat in the critically important country of Saudi Arabia. Four permanent employees had been hired, trained, and deployed that summer, and those VSOs were to stay for a one year period. The program was to be expanded to five additional countries; I understand four of them to be Pakistan, Indonesia, the United Arab Emirates, and the Phillipines. Plans were made to expand the program at the rate of five per year. But, as I pointed out in House testimony at the time, "... this is troubling, because at that rate it will take about 40 years for VSOS to be deployed worldwide, giving terrorists plenty of time to apply for a U.S. visa from countries lacking the putative protections of the program." The delay was attributable to State Department resistance to perceived encroachment on its turf, limited DHS resources, and the general lack of urgency on the part of DHS that, sadly, can be seen time after time on one issue after another.

It is unclear to me whether the program has been expanded since to additional countries. Certainly, it has yet to be expanded to virtually every country from which we issue visas, as the statute contemplated. This step should be taken urgently, provided, of course, the DHS personnel dispatched have the experience, expertise, and resources they need to be effective.

*DHS Should Continue to Insist on Meeting the Western Hemisphere Initiative Deadline*

In the area of passports, I want to commend the State Department for its efforts in this area since 9/11. The requirement that visa waiver travelers with passports issued, renewed, or extended on or after last October have machine readable passports with biometric identifiers included certainly strengthens security. And, the progress toward developing an "e-passport" for us Americans is likewise to be commended.

In terms of concerns in the area of passports, I would simply highlight one issue here. The 2004 law overhauling the nation's intelligence structure also mandated that travelers, including American citizens, entering or re-entering the United States from Mexico, Canada, the Caribbean, and Central or South America present a passport or a limited number of approved alternatives when they do so, by a date certain. The original deadline for implementation as to air travelers was this past January 1; the deadline for land and sea travelers was to be next January 1. Though Congress has worked to extend that deadline by a year, Secretary Chertoff has insisted on working to meet it. The Secretary is heartily to be applauded for this stance, and I am hopeful that the department will meet this deadline. Any unnecessary delay in doing what we can to further secure travel documents is inexcusable.

Thank you, again, Madam Chairman and members for your invitation to testify today. I look forward to your questions.

**Clark Kent Ervin**
**Director, Homeland Security Initiative**
**The Aspen Institute**
**(202) 736-1494**
**Clark.ervin@aspeninstitute.org**

STATEMENT

OF

MICHAEL EVERITT
UNIT CHIEF
ICE FORENSIC DOCUMENT LABORATORY

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
U.S. DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

**"INTERRUPTING TERRORIST TRAVEL: STRENGTHENING THE SECURITY OF INTERNATIONAL TRAVEL DOCUMENTS"**

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

ON

WEDNESDAY, MAY 2, 2007 AT 10:00 AM
226 DIRKSEN SENATE OFFICE BUILDING
Washington, DC

Good morning Chairwoman Feinstein, Ranking Member Kyl, distinguished Members of the Subcommittee; I am pleased to be here today to discuss strengthening the security of international travel documents to prevent terrorist travel. The U.S. Immigration and Customs Enforcement (ICE) Forensic Document Laboratory (FDL) is dedicated exclusively to fraudulent document detection and deterrence. The FDL is accredited by the American Society of Crime Laboratory Directors - Laboratory Accreditation Board (ASCLD/LAB) in questioned documents and latent prints. The FDL's mission is to detect and deter travel and identity document fraud in support of efforts to combat terrorism, alien smuggling, and other criminal and administrative violations. We provide a wide variety of forensic and support services to all Department of Homeland Security (DHS) components, including ICE, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), the United States Secret Service (USSS), and the United States Coast Guard (USCG). The FDL also supports other federal, state, and local agencies, as well as foreign government law enforcement and border control entities, including the Department of Justice (DOJ), Department of State (DOS), Department of Defense (DOD), the Federal Bureau of Investigation (FBI) and Diplomatic Security Service (DSS). The FDL is an integral part of a comprehensive approach to disrupting terrorist travel and works both domestically and internationally to strengthen the security of international travel documents.

The FDL is like other forensic laboratories in that it has a cadre of highly trained and experienced forensic scientists and support staff who conduct forensic examinations. These FDL employees make up the Forensic Section of the FDL and include Forensic Document Examiners, Physical Scientists (Ink Chemists), Fingerprint Specialists, Forensic Photographers, and Seized Property Specialists.

Forensic Document Examiners conduct examinations of documents to determine the authenticity of the document. If the document is deemed to be fraudulent, the examiner will determine the type of fraud, i.e., whether the document is counterfeit, has been altered, or was fraudulently obtained, and prepares a report outlining the findings. Physical Scientists (Ink Chemists) assist the Forensic Document Examiners determine the authenticity of a document by analyzing the inks used in the document. This is necessary today given the prominence of documents produced with inkjet and laser technology.

Fingerprint Examiners use the latest techniques and technologies to lift latent fingerprints from documents, document production equipment, wrappings, weapons, and other recovered material submitted to the laboratory. Using various Automated Fingerprint Identification Systems (AFIS), examiners attempt to identify individuals relevant to the investigation and then link these individuals

to evidence in the case. The FDL also has a team of Forensic Photographers who assist all FDL staff with expert photographic services. These services include capturing images of documents and other evidence under various forms of light, providing photographs and graphics for reports, and preparing court exhibits.

The Seized Property Specialists handle all of the evidence flowing in and out of the FDL each day. The FDL processes over 5,000 submissions each year. Each submission can include any number of evidence items. The proper handling and processing of evidence is of paramount importance to any forensic laboratory.

All of these employees are experts in their field and routinely testify as expert witnesses in criminal and administrative proceedings arising from ICE and other federal, state, local, and tribal agency investigations.

The training requirements for these positions are rigorous. As an example, prior to conducting their first examination on their own, Forensic Document Examiners must successfully complete an in-house 30-month training program (24 months of training followed by a six-month apprenticeship) that includes instruction on all facets of document examination, printing processes, security features, wet and dry seals, typewriter examinations, and handwriting

analysis. This comprehensive training is necessary to acquire and maintain laboratory accreditation and personnel certification. The FDL- provided training is in addition to the requirement of a Bachelor's degree. Many of the FDL Forensic Document Examiners also have Master's Degrees in Forensic Science and have obtained or are in the process of obtaining independent board certifications. The primary responsibility of the Forensic Document Examiners is to conduct examinations of fraudulent travel and identity documents submitted to the FDL. These documents are typically seized from individuals attempting to enter or remain in the United States illegally, or from fraudulent document production operations.

The FDL differs from most forensic laboratories in that it has a separate group of employees who collect and analyze information developed by the Forensic Section about particular fraudulent documents and distribute that information to the field via training, real-time support, and publications. These employees are Senior Intelligence Officers and they make up the Operations Section of the FDL. Many of the Senior Intelligence Officers working at the FDL have previously worked at large ports of entry and have extensive experience with international travelers and the documents they use.

As stated above, the FDL provides support to many DHS agencies and other federal, state, local, tribal, and foreign law enforcement and border control agencies. This support includes not only conducting forensic examinations on

material submitted to the laboratory, but also providing real-time support, providing training in fraudulent document detection and recognition, and developing and distributing numerous informational publications related to fraudulent documents, such as Document Alerts, Intelligence Briefs, and Reference Guides.

Real-time support is provided 24 hours a day, 365 days a year to assist all federal, state, and local law enforcement officers with questioned documents. Senior Intelligence Officers are on-site from 7:00 am until 7:30 pm on each workday. These officers are also on-call after-hours and on weekends with secure access to FDL systems and databases necessary to provide support. Real-time support is also provided to personnel that may have questions concerning travel and identity documents, including Department of State Consular Offices which adjudicate visa requests, and USCIS personnel who adjudicate requests for immigration-related benefits. In fiscal year 2006, the FDL received over 5,200 intelligence inquires of which more than 2,400 were from non-DHS agencies.

Document Alerts, Intelligence Briefs, and Reference Guides are produced, printed, and distributed to more than 800 law enforcement and border control agencies worldwide to assist officers in identifying fraudulent documents in circulation. Many of these publications are also posted on various DHS Internet portals to make them available to as many agencies as possible. All of these

publications are high-quality products with descriptive text and detailed graphics. The publications are designed to convey the information in a clear and concise manner, which allows the front line officer to absorb the information quickly and retain that information for use in the field.

Senior Intelligence Officers also design and provide fraudulent document recognition and detection training programs for DHS personnel and other federal, state, local and foreign law enforcement officers. This fiscal year alone, the FDL has trained more than 1,900 individuals in locations all over the world, including the United States, South Africa, El Salvador, Botswana, Jordan, Trinidad & Tobago, Kenya, Turkey, and Yemen. Of the individuals trained this year, over 200 were from CBP. The FDL also receives requests for training from state and local law enforcement agencies and from private concerns. The FDL has responded to these requests. To meet the increasing demand for these services, the FDL created "Train-the-Trainer" classes. These classes enable FDL to train persons in other agencies who then conduct fraudulent document recognition training with FDL support. The "Train-the-Trainer" program permits the FDL to expand the number of fraudulent document recognition training classes conducted each year.

The co-location of the Forensic Section and the Operations Section at the FDL allows ICE to attack the problem of fraudulent documents in a coordinated

manner and provide the necessary services to the field from a central and highly specialized facility.

Document producers and those who issue legitimate documents are in a constant battle to develop new production methods and security features to make the identification documents they issue more secure. DHS has revised and updated many of the documents associated with the immigration process. The Department of State has recently introduced a new version of the U.S. passport that includes security features intended to thwart those who would counterfeit or alter the document. However, technological advances that have made commercial-quality scanning and printing widely available have significantly increased the quality of fraudulent documents. The purveyors of fraudulent documents make full use of commercially available scanning and printing technology to manufacture better fraudulent documents, including not only hardware, but also high-quality graphic software that includes advanced techniques such as layering. Digital printing technology has been used in the majority of the fraudulent documents examined by the FDL. Sophisticated computers, software, digital scanners, and color inkjet or laser printing equipment are now routinely recovered when fraudulent document operations are discovered in the United States and overseas. For example, many of the altered passports and identity documents encountered by U.S. Forces in Iraq incorporated digitally printed components. As high-quality scanning and printing

equipment become less expensive and more readily available, digitally produced fraudulent documents become more difficult to detect.

This problem is further complicated by the increased use of digital printing technologies to create genuine identification documents. Genuine document-issuing authorities often select digital printing technologies to create or personalize genuine documents because they are less expensive than traditional methods such as offset or intaglio printing. The lower costs allow the process to be deployed to the field, rather than necessitating reliance on production centers. The result is that digitally printed fraudulent documents can be more difficult to detect by officials responsible for examining documents, such as ICE special agents, Border Patrol agents in the field, CBP officers at ports of entry, or airline security personnel overseas.

The marriage of digital technology and traditional printing methods can create fraudulent documents that are very difficult to detect. However, by incorporating security features that are specially designed to thwart reproduction by scanners or other digital equipment, such as holograms, kinegrams, specialized inks, laser etching, and new security printing techniques, documents can be made more tamper-resistant. Many of these security features cannot be duplicated easily by commercially available computer equipment and therefore make documents more secure. The development and distribution of quality documents will be expensive, as it will require replacing old document production

systems and infrastructure; however, the investment will pay healthy dividends in security.

There are many reasons for the proliferation of fraudulent documents. ICE typically sees false documents being used by illegal aliens who live and work in the United States. However, foreign nationals who seek to enter the United States and cause harm to our Nation represent another market for fraudulent documents. The quality of fraudulent documents used for international travel must be better than domestic fraudulent documents because they will be shown to people who routinely examine travel and identity documents. CBP officers inspect the documents of passengers arriving by air or sea, as well as those attempting to enter over land. Last fiscal year, CBP inspected more than 422 million people coming to the United States. In many cases, illegal migrants, criminals, and even terrorists have tried to blend in with returning citizens, legal residents, and lawful visitors by using fraudulent documents.

In January 2005, CBP created the Fraudulent Document Analysis Unit (FDAU) to collect documents, provide ports with analysis of document trends and intelligence information, and target persons being smuggled into the United States using fraudulent documents. The ICE FDL is an accredited forensic laboratory, which provides scientific examination of questioned documents, maintains a document reference library, and provides support for field investigations. CBP works cooperatively with ICE to provide training to CBP

Officers and to conduct special operations targeting travel documents in various CBP venues.

As discussed above, the problem of fraudulent documents is a perplexing one. The availability of technology to create high-quality fraudulent documents demands that the issuers of valid documents develop and use new security features and production techniques that cannot be easily duplicated. Many new security features and production techniques have been developed; unfortunately, they are not being used in many travel and identity documents issued in the United States. Recently, we have seen an emphasis on deploying electronic systems to validate documents. While the FDL supports these programs as an additional security feature, we believe these systems cannot take priority over the continued development of more secure travel and identification documents. Electronic validation systems will not always be available to the field officers, employers, or others who may need to verify a document's authenticity. When these systems are not available, the verifier of the document must be able to rely solely on the document. High-quality secure documents will stand on their own and increase the overall security of our document-based systems.

To assist in the development of high-quality secure documents, the FDL provides Counterfeit Deterrence Studies as a service to assist entities in designing new travel and identity documents. These studies are conducted by FDL teams consisting of Forensic Document Examiners and Senior Intelligence

Officers. The teams recommend document designs that incorporate security features to make them more resistant to fraud.

It is important to understand that fraudulent travel and identity documents are not only a challenging problem for the United States, but for law enforcement officials throughout the world as well. As long as identification is required to travel and obtain goods or services, criminals will attempt to produce fraudulent documents. The ICE FDL will work diligently to combat the production and use of fraudulent documents through our efforts in document examination, the development of higher-quality documents, the training of law enforcement and border control officers throughout the world, the publication of materials to alert these officers of new fraudulent trends and techniques, and providing real-time support to those responsible for detecting fraudulent documents, and by working hand-in-hand with our colleagues around the world who are engaged with us in the battle against fraudulent documents.

On behalf of the men and women of ICE, and specifically the men and women of the Forensic Document Laboratory, I thank the Subcommittee and its distinguished members for your continued support of our work.

I would be pleased to answer your questions.

9/11 Security Solutions LLC
"Matching policy with real solutions to make America more secure."

# INTERPOL KEY TO 9/11 COMMISSION RECOMMENDATIONS ON TERRORIST TRAVEL

**Janice Kephart**, former counsel 9/11 Commission and president 9/11 Security Solutions, LLC

**Statement for the Record**

May 2, 2007

**Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security**

**"Interrupting Terrorist Travel Strengthening the Security of International Travel Documents"**

U.S. support and engagement with INTERPOL is key to fully implementing 9/11 Commission recommendations on terrorist travel. The Commission emphasized international cooperation to contain terrorist travel in part in recognition of INTERPOL's border security programs. These same programs mesh with the U.S. policy to 'push our borders out'. Examples of INTERPOL's contribution to containing terrorist travel include its global police communication system; 'most wanted' color-coded notices; and lost and stolen passport /ID database (STLD).

The 9/11 Commission defined *terrorist travel* as the exploitation of border security vulnerabilities by terrorists seeking to travel anywhere in the world. This includes, for example, travel documentation manipulation, the recycling of passports, and use of travel facilitators and alien smugglers who are paid for acquiring and creating travel documentation for terrorist travel. Today's hearing is important because it not only shows Chairman Feinstein and Ranking Member Kyl's deep commitment to border security, but also this committee's recognition that secure travel documents are essential to verifying identity. Verifying identity—assuring people are who they say they are—is, in turn, essential to securing borders. Accordingly, the Commission stated:

*Exchanging terrorist information with other countries, consistent with privacy requirements, along with listings of lost and stolen passports, will have immediate security benefits. We should move towards real-time verification of passports with issuing authorities. The further away from our borders that screening occurs, the more security benefits we gain. (p. 389)*

***Recommendation: We should do more to...raise U.S. and global security standards for travel and border crossing over the medium and long term through extensive international cooperation.*** *(p. 390)*

The Commission specifically mentioned 'lost and stolen passports' because of INTERPOL's creation of its STLD and its potential to provide valuable, cost effective and timely information to further secure our borders. The Commission's language stressing 'extensive international cooperation' was used in acknowledgment of

INTERPOL's ever evolving contribution to counterterrorism and border security and INTERPOL's unique position as the only international body representing every national police force in the world.

Yet, despite 9/11 Commission recommendations and multiple opportunities for the US government to fully partner with INTERPOL in the last three years since the Commission issued its final report, our border officers still do not have INTERPOL's real time lost/stolen passport data as an automatic check at primary inspections at ports of entry. While the Swiss government has been stopping over 100 attempted lost/stolen passport entries per month using INTERPOL's database since December 2005, the U.S. government –if the Swiss statistics are conservatively extrapolated to US potential statistics—could have been denying about 10,000 such entries per month. Since December 2005, that could have been 170,000 attempted fraudulent entries potentially denied.*

Not only has INTERPOL built and continued to upgrade and expand this database—today 123 countries contribute stolen/lost travel document data with 6.7 million documents listed—the data can be delivered in two forms to deal with country-specific issues about network access and exchange of information. In addition, INTERPOL's database protects privacy by disassociating names from passport numbers, assuring that passport holders who rightfully report their passports as lost/stolen are not then criminalized in the event that their passport surfaces with an assumed or counterfeited name at a border inspection portal.

The value of INTERPOL's STLD does not end at the ports of entry, however. Verifying identities and authenticating documents is a theme that runs throughout the 9/11 Commission border recommendations and thus pertains to all elements of the U.S. border apparatus and ID document issuing authorities at the federal and state level.

**State Department**—*Visa applicants at consulates abroad.* Those seeking visas must present passports. They should be checked immediately with the STLD.

**DHS Customs and Border Protection**—*Ports of entry.* All POEs (air, land and sea) should have access to the STLD at primary inspection.

**DHS Customs and Border Protection**—*Land borders between ports of entry.* Alien smugglers are at times caught with caches of travel documents; access to the STLD could help determine whether the docs are legitimate and reported in the STLD or fakes.

**DHS Immigration and Customs Enforcement**—*Immigration enforcement.* All varieties of immigration enforcement—including worksite, the JTTF activity and ID Fraud Task Forces—will continue to benefit from access to the STLD.

**DHS U.S. Citizenship and Immigration Services**—*Immigration benefits.* My Center for Immigration Studies' September 2006 report *Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel* showed rampant abuse of immigration benefits by terrorists, including passport fraud. Since all persons applying for immigration benefits must present a passport and fraud in immigration benefits is notoriously high, an initial check of applicants' passport data through the STLD would be a boost to streamlining adjudication.

**State/Federal implementation of REAL ID Act**—*Minimum Standards for Secure Driver Licenses and State-Issued IDs.* The REAL ID Act sets out minimum standards for the issuance of state-issued driver licenses and personal IDs. For the states that seek to comply, identity verification of foreign residents will include a check of legal status. However, there is no way at this time to verify foreign passport information. Nor is there a way for state authorities to check if a US passport presented has been reported as lost/stolen. The STLD may fill that void.

**This Congress committed to implementing all 9/11 Commission recommendations in full. INTERPOL's work supports those recommendations. INTERPOL's programs should have had a solid place in U.S. border strategies and protocols three years ago, and thus should be a priority for appropriate authorizations and appropriations in this Congress. This committee should also commit to providing adequate oversight to assure the STLD provides optimum use to border personnel in the field.**

* The INTERPOL pilot in Switzerland has about 350,000 searches per month with over 100 solid hits. Assuming the conservative 2004 Customs and Border Protection numbers of about 35,000,000 persons processed per month, the SLTD would yield at least 10,000 solid hits per month.

*Janice Kephart can be reached via 911securitysolutions.com.*

Statement of
Paul Morris
Executive Director
Admissibility Requirements and Migration Control
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
Regarding
"Interrupting Terrorist Travel:
Strengthening the Security of International Travel Documents"

May 2, 2007

Good morning Chairwoman Feinstein, Senator Kyl, distinguished Members of the Subcommittee. I am pleased to be here today to discuss how the Department of Homeland Security (DHS), particularly U.S. Customs and Border Protection (CBP), is moving forward on programs that will facilitate travel, but still provide the level of security required to protect the United States. This is an enormous challenge. We share more than 7,000 miles of borders with Canada and Mexico and operate 325 official ports of entry. Each day, CBP officers inspect more than 1.1 million arriving travelers, and examine their documents, baggage, and conveyances. Last year alone, CBP welcomed over 422 million travelers through official ports of entry. During fiscal year 2006, CBP processed a record 87 million air passengers arriving from abroad by air, the second consecutive fiscal year the number of such passengers has exceeded pre-9/11 levels.

I begin by expressing my gratitude to the Subcommittee for the support you have shown for important initiatives that enhance the security of our homeland. Your continued support has enabled CBP to make significant progress in effectively securing our borders and protecting our country against terrorist threats. CBP looks forward to working with you to build on these successes.

I would also like to mention that DHS is committed to working with Secretary General Noble on the implementation of the Stolen Lost Travel Document (SLTD) system this year. CBP has taken the lead in the implementation of this program and we are currently on schedule to become the first country to use the SLTD as an integrated pre-screening tool. The SLTD will be added as one more tool available to our officers in the field. It is also important to note that DHS, including CBP representatives, are active participants in the Interpol SLTD Advisory Committee.

As America's frontline border agency, CBP employs highly trained and professional personnel, resources, and law enforcement authorities to discharge our priority mission

of preventing terrorists and terrorist weapons from entering the United States. CBP has made great strides toward securing America's borders while facilitating legitimate trade and travel and, thereby, ensuring the vitality of our economy.

Our efforts to gain operational control of our borders and push our zone of security outward enable CBP to better perform the traditional missions of its legacy agencies, which include: apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from the theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing United States trade laws. In fiscal year 2006 alone, CBP processed more than 29 million trade entries valued at $1.8 trillion, seized 2.5 million pounds of narcotics, processed more than 25 million containers, intercepted 47,951 significant plant pests, and inspected 132 million vehicles.

Since its inception on March 1, 2003, CBP has worked diligently to facilitate the flow of legitimate travelers into the United States. The vast majority of persons attempting to enter the United States through ports of entry have valid documentation and are lawful travelers. Some, however, attempt to enter the United States illegally through the use of fraudulent documents or other fraudulent means. CBP has implemented a number of complementary programs, both domestically and internationally, to combat the use of fraudulent documents and apprehend those who attempt to enter the United States illegally.

The standardization of travel documents is a critical step to securing our Nation's borders and increasing the facilitation of legitimate travelers. Currently, travelers may present thousands of different documents to CBP officers when attempting to enter the United States, creating a tremendous potential for fraud. In fiscal year 2006 alone, more than 209,000 individuals were apprehended at the ports of entry trying to cross the border with fraudulent claims of citizenship or false documents. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) addresses this vulnerability by mandating that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement a plan to require U.S. citizens and foreign nationals to present a passport or other appropriate identity and citizenship documentation when entering the United States. The Western Hemisphere Travel Initiative (WHTI) is that plan, and it will require all travelers to present a passport or other accepted document that establishes the bearer's identity and citizenship in order to enter or re-enter the United States.

The initial phase of WHTI went into effect January 23, 2007, obligating all air travelers, regardless of age, to present a passport or other acceptable secure document for entry to the United States by air within the Western Hemisphere. The implementation of the air portion of WHTI was highly successful, with documentary compliance rates of 99% and no interruption to air transportation. This high level of compliance was due to the holistic and collaborative planning approach taken by DHS and the Department of State

by working with the airline and travel industries, and before the new rules went into effect.

As early as January 1, 2008, travelers arriving by land or sea will be required to present a valid passport or other secure document, as determined by DHS. As with the air portion of the WHTI requirement, we are taking a holistic and collaborative approach to implementing these new requirements.

In partnership with the Department of State, the Department is using an additional layer of enforcement at our ports of entry. United States Visitor and Immigrant Status Indicator Technology (US-VISIT) uses biographic and biometric information to enhance the security of US citizens and visitors. US-VISIT is part of a continuum of security measures that begins overseas and continues through a visitor's arrival at a United States port of entry. In those cases where a visa is issued by the Department of State (in the biovisa program), biometrics such as digital, inkless finger scans, and digital photographs allow the DHS to determine whether the person applying for admission to the United States is the same person to whom Department of State issued the visa. Additionally, the biometric and biographic data are checked against watch lists of known or suspected terrorists, outstanding wants and warrants, immigration violations, and other criminal history information. This check verifies if an individual is the same person previously encountered by DHS and/or the Department of State, improving our ability to intercept the use of fraudulent identities and to make admissibility decisions, as well as the Department of State's ability to make visa determinations.

Biometric identifiers help us identify a visitor's identity so that we may match the visitor with his or her travel documents. Biometrics protect our visitors by making it virtually impossible for anyone else to claim their identity should their travel documents, such as a visa, be stolen or duplicated.

Non-immigrant visa holders and individuals applying for admission under the Visa Waiver Program are currently subject to US-VISIT biometric entry procedures at all port of entry environments. DHS published a proposed regulation to expand these procedures to additional classes of non-citizens. In addition, DHS has piloted biometric collection at exit over the last three years. DHS's US-VISIT Program has substantially added to CBP's screening capabilities, enhancing our ability to process travelers in a timely and secure fashion, and has had a deterrent effect to those who would seek to obtain admission illegally. US-VISIT's transition to a full ten-fingerprint collection system will further strengthen and expand our screening capabilities. Our collaborative efforts have made travel safer and more secure by allowing DHS and the Department of State to identify persons attempting to enter the United States using fraudulent identities and successfully screen individuals to determine whether they constitute a risk to national security.

In 2000, Congress made permanent the Visa Waiver Program (VWP). Each year approximately 15 million people from VWP countries enter the United States, free to travel for 90 days without a visa. To increase the security of the travel documents

presented applicants for admission under VWP, a machine-readable zone and a digitized photograph of the bearer were mandated in 2004 and 2005, respectively. In an effort to provide for secure verification of passport validity and to better detect fraudulent passports from VWP countries, e-passports were mandated in October 2006. These e-passports, which have an embedded electronic circuit chip containing biographic and biometric data, assist CBP officers in detecting fraudulent passports and passports in which the photograph was substituted or altered. E-passport document readers are now at 33 U.S. airports where 97 percent of VWP travelers enter the United States.

In an effort to extend our zone of security outward, the Immigration Advisory Program (IAP) posts officers overseas at high-volume, high-risk airports to screen passengers before they board aircraft destined for the United States. The IAP has two major objectives: to enhance the security of air travel by preventing terrorists from boarding commercial aircraft destined for the United States, and to reduce the number of improperly documented passengers traveling from or through a country to the United States. IAP teams identify high-risk and terrorist watch-listed passengers using the Automated Targeting System in coordination with the National Targeting Center (NTC), the Regional Carrier Liaison Groups (RCLG), and/or an assessment of passengers and their documentation. IAP works closely with air carriers and law enforcement authorities in host countries to ensure the proper disposition of cases involving identified high-risk passengers. In addition, IAP officers provide training to carriers and host authorities in document examination and passenger assessment.

Since the IAP became operational, more than 1,624 passengers have been prevented from boarding planes bound for the United States. Of those, nine were prevented from boarding flights because of security concerns – four were on the Transportation Security Administration (TSA) No-Fly list, and five were the subject of Terrorist Identities Datamart Environment (TIDE) records, the U.S.'s comprehensive terrorist database, with sufficient derogatory information to support a refusal of admission. In addition, 103 passengers attempting to travel with fraudulent documents were stopped, and 1,512 who were otherwise improperly documented were also intercepted. To date, the IAP has saved CBP $2.44 million in processing costs and the airlines $2.4 million in fines. Current IAP locations include Amsterdam, Netherlands (since June 2004); Warsaw, Poland (since September 2004); London-Heathrow, United Kingdom (since April 2006); and Tokyo-Narita, Japan (since January 2007). We expect to expand the IAP to include additional locations this fiscal year.

Additionally, the Carrier Liaison Program (CLP) was developed to enhance border security by helping commercial carriers to become more effective in identifying improperly documented passengers destined for the United States. The primary method for accomplishing this mission is by providing technical assistance and training to carrier staff. Technical assistance includes publication and distribution of information guides and document fraud summaries and alerts. The CLP provides training on U.S. entry requirements, passenger assessment, fraudulent document detection, and imposter identification using state-of-the-art document examination material, equipment,

and training tools. Training is delivered at U.S. ports of entry and at airports abroad by experienced CLP officers and is customized to meet the needs of specific carriers or locations based on performance analysis or emergent circumstances. CLP officers also assist carriers to develop and implement strategies to reduce travel document abuse. To date in fiscal year 2007, CBP has completed 31 training sessions – 17 overseas and 14 at U.S. ports of entry – and over 2,300 airline personnel and document screeners have been trained. CBP has scheduled training at over 40 overseas locations and 30 U.S. ports of entry this fiscal year. For fiscal year 2008, CBP anticipates additional training sessions at over 50 overseas locations and 30 U.S. ports of entry.

In December 2006, three Regional Carrier Liaison Groups (RCLGs) in Miami, Honolulu, and New York City became fully operational, in conjunction with the Office of Alien Smuggling Interdiction. The RCLGs have two primary functions: to provide a 24/7 source of information and expertise to carriers and border control authorities, and to prevent fraudulently and improperly documented aliens from boarding U.S.-bound aircraft through various targeting methods and by working with carriers and U.S. government representatives overseas including IAP officers and DHS representatives at U.S. Embassies worldwide. Recommendations are made to the carriers not to board aliens identified as fraudulently or improperly documented. Non-fraud cases involving basic documentary deficiencies, such as expired documents, are also offloaded from planes. Since the beginning of fiscal year 2007, the RCLGs have been responsible for the offload of 419 improperly documented travelers, 150 of whom were carrying fraudulent documents. This has also saved airlines the cost of round-trip transport for travelers who would be denied entry.

In January 2005, CBP created the Fraudulent Document Analysis Unit (FDAU) to collect documents, provide ports with analysis of document trends and intelligence information, and target persons being smuggled into the United States using fraudulent documents. In 2006, the FDAU received more than 34,000 fraudulent documents confiscated at ports of entry and mail facilities. Through analysis of the documents received, the FDAU provides information on trends in fraudulent documents to our officers on the frontline. This, in conjunction with continual on-the-job training, musters, and classes, gives CBP officers the expertise and knowledge to effectively detect fraudulent documents when they are presented at the ports of entry. The Immigration and Customs Enforcement (ICE) Forensic Document Laboratory (FDL) is an accredited forensic laboratory, which provides scientific examination of questioned documents, maintains a document reference library, and provides support for field investigations. CBP works cooperatively with ICE to provide training to CBP Officers and to conduct special operations targeting travel documents in various CBP venues.

In addition to the initiatives outlined above, we have been working in four areas to improve the data CBP gathers and maintains on lost and stolen passports:

- CBP has been refining the use of targeting systems to account for alterations of passport numbers by forgers attempting to defeat the watchlisting of lost and stolen documents. By modifying screening systems to search for "near-matches," in addition to the existing exact matches to passport numbers, CBP will increase its

success in identifying and interdicting lost and stolen passports that are being misused for entry to the United States.

- By accessing the Interpol SLTD, CBP will increase the data currently screened against for lost and stolen documents. CBP has completed a pilot with Interpol, which yielded technical data, hits against SLTD for evaluation, and issues that will need resolution to effectively utilize the SLTD at ports of entry. CBP is working with Interpol on this connection now. Secretary Chertoff has made linking with SLTD a Departmental goal in 2007. DHS is currently negotiating a memorandum of understanding with Interpol, so that CBP can continue to receive and utilize this important information. Interpol data will supplement existing data in the border screening system and serve as yet another resource for frontline officers.
- Since September 2005, the U.S. and Australia have been involved in a Regional Movement Alert System (RMAS) pilot. In March 2006, New Zealand joined RMAS with the U.S. and Australia. This tri-lateral pilot enables participating Asia-Pacific Economic Cooperation (APEC) economies to access data on lost, stolen, and otherwise invalid travel documents in real time, without the necessity of pooling data in a central database and ensuring that the most current data is always available. Based on the success of this pilot, other APEC economies have expressed interest in joining and expanding the network of available information. This initiative has proven particularly adept because it links the passport-issuing authorities with the border agencies—raising the level of confidence in the "hits" and enabling real-time communication between agencies as they make admissibility determinations. This level of communication is unique with regard to lost and stolen passport screening.
- CBP is working with the DHS Office of International Enforcement, which administers VWP policy for DHS, to become the first point of intake for lost and stolen passport information. This would ensure that this critical data is immediately directed to the border screening system.

CBP is committed to continuing work with Interpol to connect SLTD as one more resource for our frontline officers. 'We are committed to this task and are working with Interpol, through U.S. National Central Bureau on procedures and systems to support implementation. This implementation includes the first time the SLTD will be available anywhere in the world as a fully integrated pre-screening tool, and not just a tool used after arrival. We believe that this will accomplish the dual goals of facilitating legitimate travel, while ensuring sufficient time to coordinating potential SLTD hits with Interpol.

It is important for you to know that the border screening system used at all ports of entry today holds more than 3.4 million lost and stolen passport records. This data, which comes in large part from the Department of State, serves a long-standing mission of the border agency—the detection of lost and stolen passports. Officers are trained to identify mala fide travelers from those who have been victims of theft or have simply misplaced their passports. CBP works assiduously to ensure that legitimate persons are not unduly delayed while using every available resource to identify suspect persons and equip frontline officers with the training, resources and data points necessary to enable swift and accurate detection of suspect persons and documents. Additionally, CBP

works in coordination with the DHS Office for Civil Rights and Civil Liberties to facilitate legitimate travelers and prevent unnecessary delay by incorporating new programs, like the DHS Traveler Redress Inquiry Program, to ensure our law enforcement databases are accurate.

Madame Chairwoman, Senator Kyl, Members of the Subcommittee, I have outlined today some of the ways that CBP and DHS detect fraudulent documents at the border, while ensuring the identification and verification of citizenship of each applicant for admission. With the continued support of the Congress, CBP will continue to protect America from the terrorist threat while also accomplishing our traditional missions in immigration, customs, and agriculture and balancing our enforcement missions with the need to effectively facilitate the flow of legitimate trade and travel. I appreciate this opportunity to testify before you and would be happy to answer any questions that you may have.

**SENATE JUDICIARY HEARING OF THE JUDICIARY COMMITTEE, SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY**
**WASHINGTON DC, (USA)**
**2 MAY 2007**

**ORAL STATEMENT**

**BY**

**RONALD K. NOBLE**
**SECRETARY GENERAL**
**ICPO – INTERPOL**

**2 May 2007 – 10h00**
**US Senate Dirksen Building**
**Washington, D.C.**
**USA**

**Oral Statement of Ronald K. Noble, Secretary General of Interpol**

**Before The Senate Judiciary Committee**
**Subcommittee on Terrorism, Technology, and Homeland Security**

**Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents**

**2 May 2007**

Chairman Feinstein, Ranking Member Kyle, Distinguished Members of the Subcommittee, Good Morning.

Al Qaeda and Al Qaeda-inspired terrorists are trying to kill and harm the world's citizens.

They are doing so right now.

Depending on the group, the circumstances, and the opportunities, they would love nothing more than to kill US citizens and the friends of US citizens on US soil.

But, they also love targeting US embassies, US military vehicles and personnel, US businesses and US citizens anywhere they might be found in the world.

They know the combustible ingredients that would attract worldwide attention – "Al Qaeda strikes US targets."

There are those who blindly take comfort in the fact that the US has not been hit hard within its borders since September 11, 2001. I know one high-ranking US Government official who was so dedicated and committed to protecting US citizens on US soil that, on any given day, he could tell you how many days had elapsed been since September 11, 2001.

In my capacity as Interpol's Secretary General, I take no comfort, absolutely no comfort, in the fact that Al Qaeda has not struck the US within US borders since 9/11. Of course, we all should be thankful that no innocent lives have been taken or harmed, but viewing the absence of terrorist attacks on US soil for a certain amount of time as a success is the wrong approach. It can give one a false sense of comfort, and it can make you falsely conclude that Al Qaeda cannot strike – as opposed to, has not chosen to strike.

For me, I use different points of reference in terms of time and comfort. I see the time since the last terrorist attack as a time bomb that must be defused before it explodes. My point of reference is not the number of days between September 11, 2001 and today, but the number of days between the first World Trade Center attack by Al Qaeda on February 26, 1993 and the second set of attacks on September 11, 2001.

Al Qaeda waited and prepared for more than 8 years (3,119 Days to be precise) before striking the US again.

This means that we can and should not take any real comfort from the fact that the US has not been hit again since 9/11.

As I said, I use time bombs as my points of reference. I see members of Al Qaeda, and terrorists linked to or individuals who are or may be inspired by Al Qaeda, as human time bombs. They have almost 200 countries in the world where they can operate, where they can plan or prepare, through which they can travel.

The challenge for our generation, and maybe for generations to follow, is how can we, individually and collectively, prevent these vicious terrorists from killing or harming us and those we love and represent.

Since September 11, 2001, Interpol has been regularly transforming itself to help each and every one of its member countries disrupt, prevent, investigate, track down, apprehend, and prosecute terrorists the world over. We have done so by thinking about this issue almost every minute of every day; by meeting and consulting with our member country National Central Bureaus, and law enforcement officials from around the world; by engaging elected officials, appointed government officials; reporters; business leaders, and citizens in discussions about what they see as weaknesses in their country's or other countries' anti-terrorist efforts.

We then have tried new approaches; received constructive (sometimes harsh) criticism; we have gone back to the drawing board; we have identified countries willing to pilot some of our ideas; we have shared the results with wider groups of member countries. Eventually, we have found the best building blocks to put it in place – always willing to modify or refine as we went along.

We now have an approach that we have been using since 2002 as an investigative tool for investigators of terrorism and serious crime and that we expanded in December 2005 to become an essential additional border control tool for law enforcement at border points of entry and indeed anywhere a person's passport or travel document would be examined by a local, state or federal police officer.

The best way to describe Interpol's state-of-the-art approach to enhancing the border security of each and every country is to visualize tripwires interconnecting around the globe and in the paths of terrorists and other dangerous criminals. Depending on the type of wire that is tripped, either a silent or loud alarm is triggered, alerting law enforcement that they might have a person of interest to another law enforcement agency somewhere in the world standing right in front of them.

Interpol's tripwire system is in place and is working.

Between 2000 and 2006, the number of annual checks in Interpol's nominal database has increased nearly tenfold, from 81,034 to 703,000 searches. Between 2000 and 2006, the number of Red Notices issued annually by Interpol has nearly tripled, from 1,077 to 2,804. The number of diffusions (which are like "Be On The Lookouts" in the US) issued annually through Interpol has more than doubled, from 5,333 to 12,212. The number of annual arrests of individuals who were subject to Interpol Red Notices or diffusions has surged from 534 to 4,259, a 698 per cent increase. In total, more than 18,000 international criminals who were subject to Interpol Red Notices or Diffusions have been arrested since 2000.

Now, despite the success that Interpol has achieved in terms of gathering and sharing information from a wide variety of countries on suspected terrorists and on stolen travel documents, there seems to be intractable resistance in some corners of the US's and other countries' bureaucracies to using information coming from global sources. These entities prefer to use the way that was in place prior to the first World Trade Center bombing in 1993 and the September 11, 2001 terrorist attacks.

As I said in my written testimony, if this view continues to reflect the attitude of those whom we expect to protect us from the next wave of terrorist attacks, we are in serious, and I repeat serious, trouble as a world community.

Can you just imagine for one second what ordinary citizens on the street would say, right now, before a terrorist attack, if they knew that the US Customs and Border Protection Agency let dangerous criminals and terrorists into the US possessing passports that were reported stolen and lost to Interpol by the member country that issued the passport.

Now, God forbid, try to imagine what any of us could say to the family members of any person who was murdered by someone who entered the US using a stolen passport, which stolen passport had been stamped by a US Customs and Border Protection Officer whose agency did not make available to the officer the possibility of screening that passport against Interpol's Stolen and Lost Travel Document database.

Interpol has a network of 186 member countries police services; we have developed a secure global police communications system that connects these countries on a real time basis; we have collected information on over 14 million stolen and lost travel documents, including nearly 7 million stolen passports. We have responded to honest feedback saying that we needed to invent a way to give border control officers instant access to this information by inventing a way to do so. Please help us find a way to persuade border control agencies in the US and around the world that they should consult this database before allowing someone to enter or cross their borders.

I close by saying on the record that I have traveled to 107 countries as Secretary General, and I am absolutely convinced, without any hesitation, that there is no governmental structure like the elected representatives of the people that can compel a bureaucracy to change in the best interests of the safety and security of the people.

I implore you to do so here in the US, but also to help Interpol do so around the world!

**SENATE JUDICIARY HEARING OF THE JUDICIARY COMMITTEE, SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY**
**WASHINGTON DC, (USA)**
**2 MAY 2007**

**STATEMENT**

**BY**

**RONALD K. NOBLE**
**SECRETARY GENERAL**
**ICPO – INTERPOL**

**2 May 2007 – 10h00**
**US Senate Dirksen Building**
**Washington, D.C.**
**USA**

**Statement of Ronald K. Noble, Secretary General of Interpol**

**Before The Senate Judiciary Committee**
**Subcommittee on Terrorism, Technology, and Homeland Security**

**Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents**

**2 May 2007**

## I. Terrorists Have Been Exploiting A Gaping Hole in Global Security Since At Least 1993

As the 9/11 Commission found -- "For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack."

On September 1, 1992 – almost 9 years to the day before the September 11 terrorist attacks on the US and the world – Ramzi Yousef, the convicted mastermind behind the first World Trade Center bombing in 1993, used a stolen blank Iraqi passport to reach the US where he claimed asylum upon his arrival. He flew here with co-conspirator Ahmad Ajaj, who possessed a stolen Swedish (visa waiver country) passport.

Almost a decade later, history repeated itself with the deadly terrorist September 11 attacks targeting the World Trade Center again and other vital US interests. According to the 9/11 Commission, two of the 9/11 hijackers entered the US using fraudulent passports, and six others may have also used fraudulent passports. Even with the heightened security following 9/11, there remain documented cases of foreigners entering the US using falsified stolen passports – including at least 20 cases involving passports that had been stolen (as part of a batch of 708 blank passports) in a city that was home to an al Qaeda cell that "played a significant role in providing financial and logistical support for September 11th terrorists." See DHS OIG-05-07 (December 2004).

Terrorist use of fraudulent travel documents was one of the most dangerous gaps in global security back around the time of September, 2001. Unfortunately, it still is today.

Indeed, even today – 5½ years after 9/11 – terrorists and other criminals can all too freely travel the world to plot and execute their attacks and commit other crimes, while concealing their identities through the use of fraudulent passports. Fraudulent passports have been used by, or found in the possession of, terrorists involved in recent attacks, including the 2004 Madrid bombing, and the 2005 London bombing (attacks that killed 243 people and injured over 2,400 others).

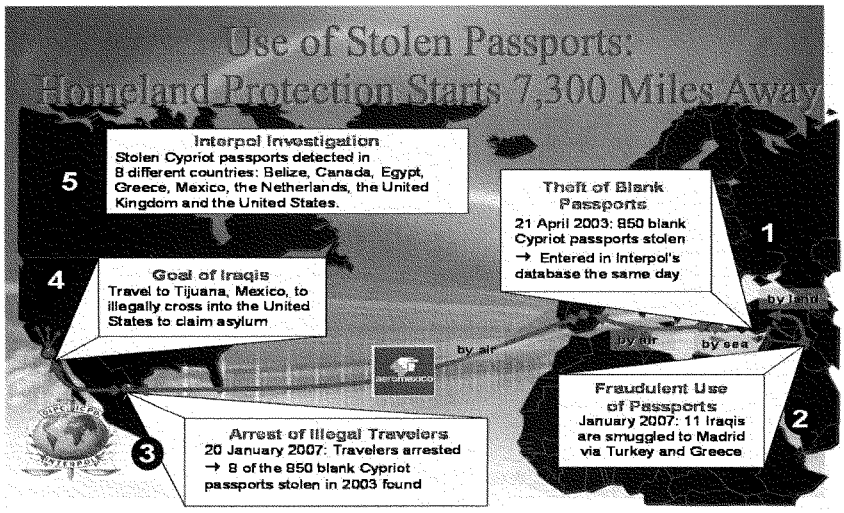
Terrorist use of fraudulent passports is the subject of two recent reports issued by the US Government Accountability Office, one issued on 7 September 2006 (GAO-06-1090T), and the other issued on January 24, 2007 (GAO-07-375). The 7 September 2006 GAO Report found that stolen and lost passports are "prized travel documents among terrorists" and "officials acknowledge that an undetermined number of inadmissible aliens may have entered the US using a lost or stolen passport." The 24 January 2007 GAO Report reiterated these findings.

Terrorists and other criminals know they can use falsified stolen passports with little chance of detection. Stolen passports, particularly those stolen in blank form, present the greatest threat because they can be made into fraudulent passports that are among the most difficult to detect.

A recent example will illustrate this.

On 20 January 2007, eleven individuals who had arrived on a flight from Spain were stopped at the Monterrey airport in Mexico, after a vigilant border officer became suspicious of their reasons for visiting Mexico. The ensuing investigation revealed that the 11 individuals were, in fact, Iraqis who had traveled from Iraq, through Turkey and Greece by land and sea, and then by air to Spain and Mexico, with the ultimate goal of crossing into the US illegally, allegedly to seek asylum – just like Ramzi Yousef in 1992.

Interpol later became involved, and discovered that the Cypriot passports that were used by 8 of the Iraqis were registered in Interpol's stolen travel document database as part of a lot of 850 passports that had been stolen in blank form in 2003. But the Mexican border security system is not connected to the Interpol database, so their immigration officers did not know this.

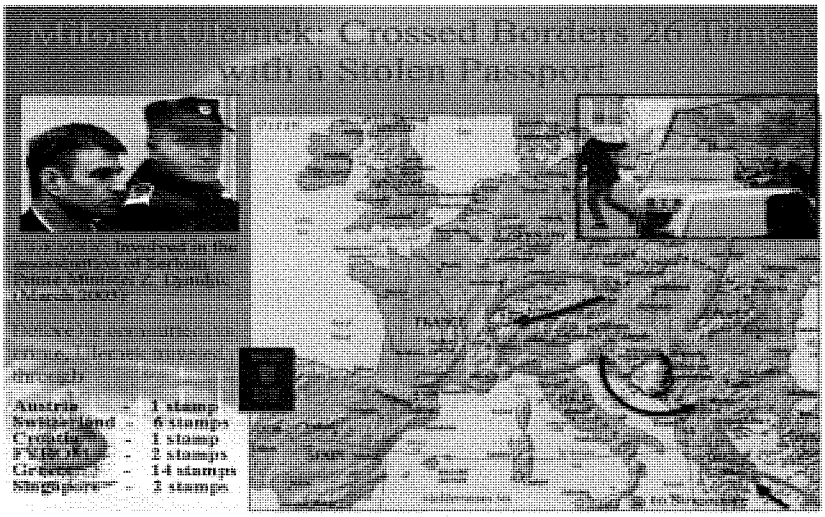



While preliminary investigations suggests that these eleven Iraqis do not appear to have been terrorists, this example illustrates, among other things, that those involved in the business of supplying fraudulent stolen passports to those who seek to travel under false identities know they can do so with little chance of detection. And they are right about this – there is little chance that the fraudulent passports will be detected in a systematic fashion throughout the world. Indeed, here we have a case where passports were stolen in 2003, and they were brazenly used years later in 2007, and the reason the users were not successful is because a border guard happen to become suspicious of their travel story.

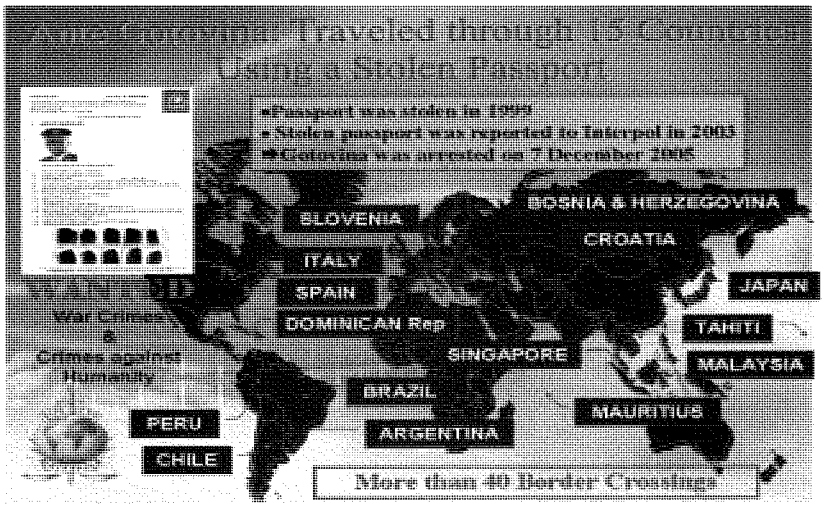
There are many examples where people have used stolen passports to travel for terrorist or other criminal purposes. Wali Khan, convicted in the Manila airline bombing plot with Ramzi

Yousef, possessed a stolen Norwegian (visa waiver country) passport. Though Khan never traveled to the US, his case demonstrates the need for the US's vigilance to go beyond its borders in order for the US and its citizens to be protected from terrorist attacks. The planning and preparation of terrorist attacks targeting the US can and do occur all over the world.

Another example of the worldwide threat posed by stolen blank passports involves one of the chief suspects (Milorad Ulemek) currently on trial for the assassination of Serbian Prime Minister Zoran Dindic in 2003. Ulemek used a falsified stolen Croatian passport to travel extensively in allegedly planning and carrying out the assassination. After he was arrested, it was discovered that his fraudulent stolen passport had been stamped 26 times by law enforcement officers in 6 countries.




Another recent example involves a wanted War Criminal, Ante Gotovina, who was wanted for war crimes and crimes against humanity. He had no problems using a falsified stolen passport to travel through 16 countries throughout several years, making over 40 border crossings, before he was finally captured in 2005. He was captured based on an Interpol Red Notice, his falsified stolen passport having never been detected by law enforcement officers at the borders, when it easily could have been detected using Interpol's Stolen and Lost Travel Document database.



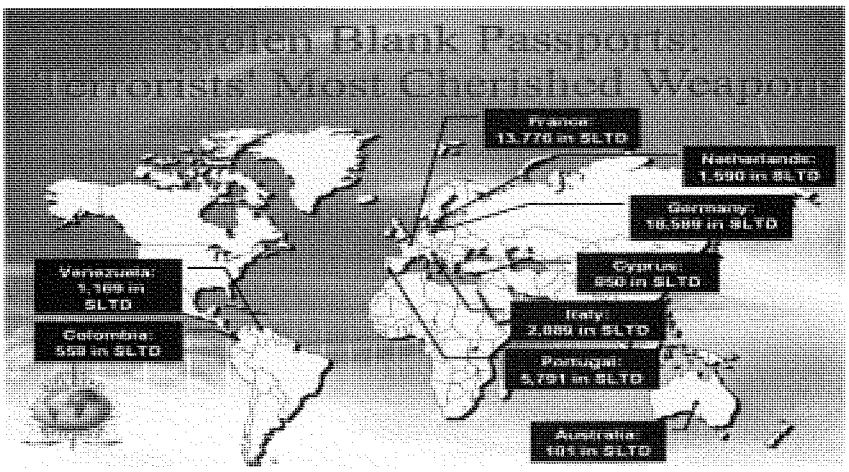

These examples reinforce the view that unless there is a systematic way for countries' law enforcement officers to determine whether passports have been reported stolen, all countries risk that more terrorists and other dangerous criminals will use them to travel the world freely in order to plan and perpetrate deadly attacks. Not just terrorists, but also other varieties of dangerous criminals regularly use fraudulent stolen passports to conceal their identities in order to travel internationally undetected, plan and commit crimes, and evade justice.

## II. Interpol's Response: Creation of the Global Database of Stolen & Lost Travel Documents and the Technology to Connect it to Border Systems Worldwide

To address this threat, Interpol created a global database of stolen and lost travel documents (the SLTD database), as well as the technology needed to make this database accessible to officers around the world at airports, seaports, other border entry points, and, indeed, at any field location. This technology, which we call MIND/FIND, is revolutionizing the way countries conduct border security.

### A. The Interpol SLTD Database

Recognizing that there was no single global repository of information on stolen and lost travel documents, Interpol launched its SLTD database in 2002. The database began with approximately 3,000 passports reported stolen from 10 countries. It has since grown astronomically to 14.4 million stolen and lost travel documents from 123 countries. This includes 6.7 million passports and 7.7 million other types of travel documents (identity cards, visas, etc.). Included within the passports are many that were stolen in blank form, which pose the greatest threat because they can be made into fraudulent passports that are among the most difficult to detect. Below is a sampling of some the blank passports in the SLTD database. (With 63 Interpol member countries still not reporting stolen or lost passports to Interpol, this list is obviously incomplete.)




Through Interpol's secure global police communication system (called I-24/7), which is deployed throughout 185 countries, officers can query the SLTD database and instantly determine whether a travel document has been reported to Interpol as stolen or lost. This access is available at the Interpol National Central Bureau (NCB) located in each country. Indeed, Interpol encourages all of its member countries to extend this access beyond their NCBs – to all of their law enforcement agencies (especially at points of entry), and a growing number of countries are doing so.

It should be noted that there are no privacy issues regarding the SLTD database, as it contains no personal information, such as the name, date of birth, or any other identifying information of the lawful bearer. Such information remains with the country that issued the passport. The purpose of Interpol's database is to permit the rapid and systematic identification of potential criminals and security risks. Once the initial identification has been made, the person is moved from primary to secondary inspection where the member countries can immediately engage in bi-lateral discussions to determine who the bearer of the passport that has been reported lost or stolen really is. If and when the consulting of Interpol's SLTD database occurs prior to the person's boarding of a flight, the bi-lateral country consultations can occur before the traveler reaches his or her final destination point.

As stated above, Interpol's SLTD database collects information related to the document itself (i.e., the number of the document, the type of document, the issuing country, and the date of the theft or loss), not to the bearer of the document. Interpol intentionally designed its database in this regard in order to avoid complaints that the personal data of innocent individuals would be made a part of Interpol's database. Interpol's approach has allowed its database to be populated with data from countries that otherwise would never haven been willing to share their data globally. This is a common thread to Interpol's philosophy. We try to find ways that encourage countries to share police information. Interpol's approach has proved valuable and successful.

To date, the Interpol SLTD database has been endorsed as an effective law enforcement tool by numerous regional Chiefs of Police networks throughout the world, and is strongly supported by numerous international organizations, including the United Nations Security Council, the G8,

the European Union, the Asia-Pacific Economic Cooperation (APEC), the Organization for Security and Cooperation in Europe (OSCE), and the International Civil Aviation Organization (ICAO). UN Security Council Resolution 1617 (2005) specifically urges countries "to ensure that stolen and lost passports and other travel documents are invalidated as soon as possible and share information on those documents with other member states through the Interpol database."

It is important to note at this point that Interpol respects the sovereignty of each member country as it relates to its SLTD database (and all Interpol databases). Only the sovereign country that issues the passport is authorized to enter, modify, or delete its own stolen and lost travel documents data in Interpol's database. The passport issuing country is the owner of such information. And the passport issuing country can place restrictions on which countries it will allow to see its data. These are important points to stress.

Interpol is not blind to the realities of the world in which we find ourselves. It will likely never be the case that all countries will wish to share all of their law enforcement related information with all other countries. Since the terrorists are continuously planning to kill and harm innocent people, Interpol tries to find flexible ways for countries that wish to share certain law enforcement information to do so. Taking the US as an example, it regularly chooses not to share law enforcement information with countries such as Syria, Iran, and Cuba – so Interpol's rules permit it to exclude those countries. Certain European countries give Interpol an itemized list of countries that can receive certain types of information, and not other types of information. It sounds complicated, and it is. But, Interpol has found that unless it respects a country's sovereign right to choose what to share and with whom to share it, a country will not be willing to share information.

Here are two examples that prove that even countries that are perceived as "enemies" can at times have common law enforcement goals: (1) The first country in the world to seek the arrest of Osama Bin Laden internationally for deadly terrorist attacks was Libya, at a time when Libya and the US had no formal diplomatic relations, and well before the deadly September 11 terrorist attacks (Libya did so via an Interpol international wanted person's notice – an Interpol Red Notice); (2) Ramzi Yousef (the convicted mastermind of the first World Trade Center attack) entered the US claiming asylum using a stolen Iraqi passport in 1992, when the US and Iraq were so-called enemies. These two examples make clear that it is against a country's own national security interest and safety to ignore law enforcement related information coming from a perceived "enemy." Instead, each country should make an independent determination about whether and how much to credit information coming from a perceived "enemy." Interpol's philosophy and way of working facilitates each and every member country's ability to do so.

### B. The Interpol MIND/FIND Connection Technology

While usage of the SLTD database by NCBs and other law enforcement agencies may be helpful to investigators who want to check a specific suspicious travel document as part of a particular investigation, such usage will not prevent terrorists and other criminals from entering a country. In order to accomplish that, the SLTD database must be used by border control officers to screen passports at airports and other border entry points.

For example, in the case of Milorad Ulemek discussed above, the falsified stolen passport he used was one of 100 blank passports stolen from the Croatian Consulate in Mostar (Bosnia and Herzegovina) in April 1999, and the theft had been reported to Interpol. Although the SLTD database had not yet been created at the time of theft, it was already in place when Ulemek started travelling to plan for the crime with which he has been charged. Ulemek was never

stopped at any of his 26 border crossings because the passport was not checked against Interpol's SLTD database at those border entry points. Similarly, in the case of Ante Gotovina, the fraudulent stolen passport – which, incidentally, came from the same batch of 100 Croatian passports stolen in 1999 – which was used to travel throughout 16 countries was also listed in the Interpol SLTD database, but the subject countries were not checking passports against that database at their border entry points.

The fact is that Interpol's database was initially designed as an investigative tool, not as a border protection tool. The USNCB and US law enforcement should be credited with bringing this weakness to Interpol's attention. The USNCB consulted with the relevant US law enforcement entities to learn what they liked or disliked about Interpol's SLTD database. Based on this dialogue, Interpol learned that certain US law enforcement agencies complained that entering passport numbers manually at points of entry would be too time consuming.

This complaint led Interpol to re-conceive the purpose of its SLTD. Our member countries wanted a border control tool as well as an investigative tool. Without the US' support it would be virtually impossible to get global acceptance of its SLTD database as a valuable law enforcement tool. Without such acceptance, countries (including the US) would try to develop incomplete bi-lateral approaches to the problem of criminal use of stolen travel documents, which in Interpol's view, is the greatest threat to global security. Consequently, dedicated staff at Interpol's General Secretariat in Lyon, France developed technology that would allow law enforcement officers to instantly check Interpol's SLTD database at airports, seaports, other border entry points, and, indeed, at any field location.

Put another way, the honest and accurate feedback that we received (principally from US law enforcement) resulted in revolutionizing the way that border control can now be effectuated at points of entry throughout the world. While it is never pleasant to receive negative feedback, such feedback can provide great opportunities for change. Receiving and responding to such criticism in the past has helped make us a stronger and more relevant law enforcement organization in fighting terrorism and other forms of serious crime. Interpol is innovative and responsive to the needs of its 186 member countries.

To respond to these needs, Interpol developed technology that enables law enforcement to check Interpol's SLTD database at all border entry points. There are no extra steps – the same swipe of the passport automatically checks the Interpol database in parallel with the check of the national database. This technology (called MIND/FIND) has transformed the way that countries conduct border security.

The MIND/FIND technology refers to two different ways of connecting the SLTD database to border control systems. The choice is based on a country's technical infrastructure.

- The FIND system (which stands for Fixed Interpol Network Database) allows a country's national system to search Interpol's SLTD database in Lyon, France over the internet through a secure virtual private network (Interpol's I-24/7 global police communications system). When the passport is swiped, the system will check the Interpol SLTD database in parallel with the national database.

- The MIND system (which stands for Mobile Interpol Network Database) allows a country's national system to search a copy of the Interpol SLTD database that is located within the country. Interpol provides the country with an encrypted copy of the database on a storage device (called a MIND Box). When the passport is

swiped, the system will automatically check the Interpol SLTD database that is stored in the MIND Box in parallel with the national database. The copy of the database is automatically updated by Interpol, whenever the MIND Box is connected to Interpol through I-24/7. To prevent countries from using stale data, the Mind Boxes become inactive if not refreshed on-line within a certain number of days.

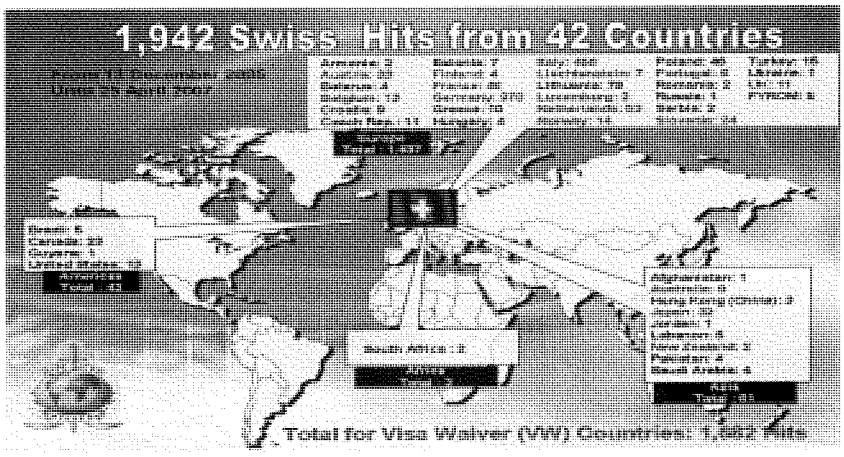
At present, MIND/FIND is used primarily to access the Interpol SLTD database and the Interpol Stolen Motor Vehicles (SMV) database, but work is underway to also include other databases.

### C. MIND/FIND In Action

The MIND/FIND technology has dramatically changed the way countries conduct border security. This becomes clear when one compares the use and results of Interpol's SLTD database today with the use and results in 2003, the first full year in which the SLTD database was in operation. Thanks mainly to MIND/FIND, law enforcement officers now perform far more SLTD searches each and every day than in the entire year of 2003, and they obtain more hits each and every month than in the entire year of 2003.

#### 1. Switzerland – The First Country to be Connected

On 13 December 2005, Switzerland became the first country to implement the MIND/FIND connection technology, enabling some 20,000 Swiss officers to screen passports at border entry points. Using this technology, Swiss officers conduct on the order of 300,000 to 400,000 database searches per month. And these searches get results – each month the Swiss detect over 100 persons attempting to enter their country using passports that had been reported stolen/lost.




The Swiss numbers bear witness to the urgent need for all countries to implement Interpol's MIND/FIND border security tool. A small, but growing number of countries are beginning to recognize this, but until every country actually implements this border security tool there will remain a dangerous gap in global security.

Based on the results achieved by Switzerland, other countries have expressed their interest in deploying the MIND/FIND connection technology to their border systems, and are in various stages of assessment, testing, or implementation. France, for example, began screening passports at Charles de Gaulle Airport in Paris on 8 June 2006. It has been conducting on the order of 140,000 searches per month, resulting in 18 "hits" a month. In April 2007, France extended the connection to 6 international train stations, 11 international seaports, and 21 airports.

Other countries, such as Algeria, Belgium, Bosnia and Herzegovina, Brazil, China, Croatia, Czech Republic, Denmark, Finland, Indonesia, Lithuania, Italy, Macedonia, Montenegro, New Zealand, Norway, Portugal, Saudi Arabia, Singapore, Spain, Turkey, the United Kingdom, and the United States, are in various stages of assessment, testing, or implementation of a MIND/FIND system.

The US has not yet begun screening passports against the Interpol SLTD database at its border entry points. The US has successfully tested the MIND/FIND system in order to ensure its functionality. DHS Secretary Michael Chertoff has stated that DHS has set a goal of being able to screen all passports against the Interpol SLTD database at all points of entry by the end of 2007.

**2. The Caribbean – The First "Region" to be Connected**

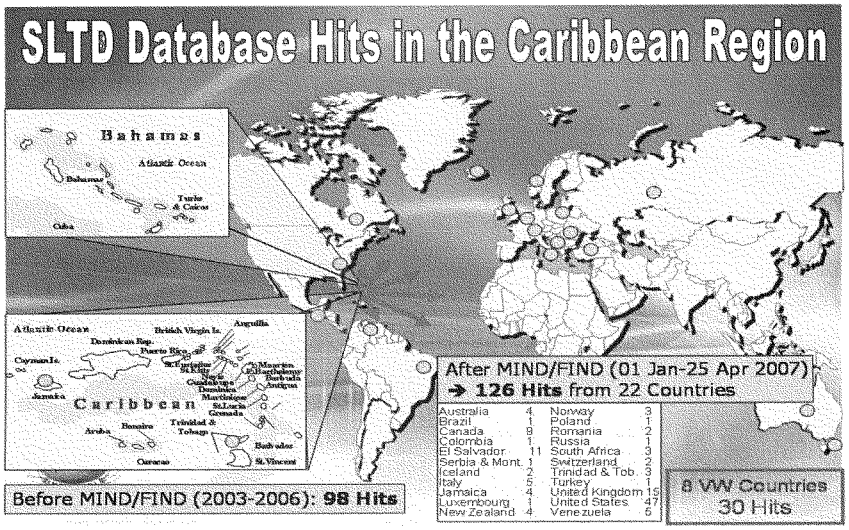
The Cricket World Cup was held in the Caribbean region from March through the end of April 2007. As Secretary General of Interpol, I took the decision to respond to the Caribbean's request for assistance in providing security for the Cricket World Cup – even though Interpol had no budgeted funds to do so, and even though I knew nothing about cricket. By consulting with Interpol member countries and doing a little reading, I learned that the Cricket World Cup is the 3d largest viewed sporting event in the world. It attracts millions of television spectators and some 100,000 visitors. It could have been a prized target for terrorists. And it is apparent that enhanced border security in that region enhances the security of the US (as the White House has observed through its "Third Border Initiative" that the Caribbean is often a gateway into the US), and it also enhances the security of every other country in the world.

The security issues were particularly challenging due to the fact that the games were hosted in multiple countries (nine in total) throughout the region. Despite its small size in terms of population, and despite the challenges of reaching agreement among so many sovereign nations, the Caribbean countries demonstrated the political will, the commitment, and the dedication to achieve what most of the world would have thought impossible. The Caribbean became the first region in the world to integrate a national and regional border control structure with Interpol's global SLTD. Some of these countries have even started performing advanced passenger manifest clearance procedures using Interpol's nominal database.

Thanks to the strong commitment of ministers, commissioners, chiefs of police, NCBs, and other members of the law enforcement community throughout the region and the world, all of the nine host countries (Barbados, Antigua & Barbuda, Grenada, St Kitts & Nevis, St Lucia, Trinidad & Tobago, St Vincent & The Grenadines, Guyana, and Jamaica) and two other countries in the region (Bahamas and Dominica) were able to screen passports against Interpol's SLTD database during the event, and can continue to do so now that the event is over.

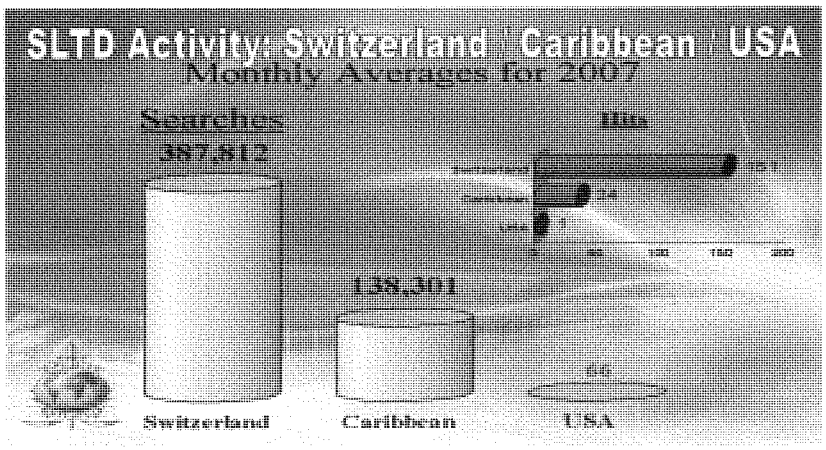
The results were nothing short of amazing, and are worthy of special recognition by the US and indeed all countries. While the total number of searches in Interpol's SLTD database by the

nine host countries amounted to just 1,218 searches in all the years prior to 2007, once the MIND/FIND system was running this number skyrocketed to 45,000 during the first month of 2007 alone. These searches led to 9 hits on passports that were reported stolen or lost. Through 25 April 2007, the Caribbean countries conducted nearly 500,000 searches, resulting in 126 hits.




Let us take a look behind one of those hits, in order to illustrate how the system actually enhances security in the Caribbean region. On 16 March 2007, immigration officers at the Barbados international airport checked a passport against Interpol's SLTD database, which resulted in a hit, indicating that the passport had been reported stolen or lost. The subject was interviewed and stated that the passport was his and that he had never reported it as stolen or lost. He further stated that he was a Nigerian by birth, but gained Venezuelan citizenship after living in Venezuela for seven years. After investigation, however, it was discovered that the passport was stolen, and the man was arrested.

Below is a graph showing the positive impact of the MIND/FIND technology on national law enforcement activity based on the MIND/FIND deployments in Switzerland and the Caribbean.




The significant difference in the activity levels is due to the fact that the SLTD database is now accessible through the MIND/FIND connection technology in Switzerland and the Caribbean, but not yet in the US.

Just this week Barbados' Deputy Prime Minister, Mia Mottley, requested additional staff from Interpol to ensure that the Caribbean's Joint Regional Command Center that was created for the Cricket World Cup could continue its fine work beyond this event. It wishes to continue the screening of passenger manifests against Interpol's global database as well as national and regional databases in the Caribbean. As has been made clear on a number of occasions, a more secure Caribbean region will lead to a more secure US. While Interpol may be able to provide temporary assistance to this initiative, the US can make the Caribbean's efforts more successful by supporting the Caribbean in ways that Interpol could never do on a long term basis. Doing so would benefit the Caribbean, the US, and the entire world's anti-terrorist and anti-crime efforts.

## III. Implications For The Visa Waiver Program

The threat of terrorists and other criminals entering the US through the use of falsified stolen and lost travel documents is particularly acute in relation to the US Visa Waiver Program. As a recent GAO Report found, "lost and stolen passports from visa waiver countries are valuable travel documents for terrorists, criminals, and others who are seeking to hide their true identities to gain entry into the country." GAO-07-375 (January 24, 2007).

When people travel to the US using passports from visa waiver countries, they are not subject to the scrutiny of having to apply for and obtain a visa. This means that terrorists and other criminals know that if they buy passports that have been stolen or lost in these countries, then they can falsify those passports and use them to enter the US without being subject to any scrutiny from any US consulate. Consequently, such passports represent a particularly dangerous threat to US security. In fact, the 24 January 2007 GAO Report says that "experts consider it the greatest security problem posed by the Visa Waiver Program." And the facts on the ground bear this out.

Of the 288 database hits that the US obtained in 2006 by searching passports against the Interpol SLTD database, 140 were on travel documents from visa waiver countries (49% of the hits). For the same period (2006), of the 2,543 hits obtained by all the countries, 1,569 were on travel documents from visa waiver countries (62% of the hits).

To mitigate this danger, the 7 September 2006 GAO Report and the 24 January 2007 GAO Report recommend (i) the adoption of legislation that would require all visa waiver countries to provide the US and Interpol with data on all their stolen and lost passports, and (ii) the screening of all passports against Interpol's SLTD database at all points of entry.

These recommendations are the two main ingredients of an effective passport screening system. The database must have the stolen and lost travel document numbers, and passports must be screened against the database at border points of entry.

It should be noted again that there are no privacy issues regarding the SLTD database, as it contains no personal information. Only information relating to the document is stored in the database (document identification number, issuing country, type of document, whether it was stolen or lost in blank form, and any optional information regarding the theft/loss). And since a travel document does not belong to an individual, but is the property of the issuing country, there is no privacy issue with transmitting and storing this document related information.

It should also be noted that with respect to non-visa waiver countries, the US could significantly enhance its security by connecting the Department of State to the Interpol SLTD database, so that US consulates around the world could use this tool in assessing visa applications.

## IV. Rolling out MIND/FIND Worldwide

The US and every other country has an interest in seeing that the MIND/FIND technology is implemented not just in their own country, but throughout the world. It has been recognized the world over that the defense of any one country begins beyond the border, not at the border. Rather than viewing one's border as the first line of defense, it should be viewed as the last line of defense. Interpol firmly believes that internal security is intrinsically linked to international security. Stopping terrorists outside the US can prevent them from appearing at the US' doorstep.

Let me say on the record at this point, that the US and the US Department of Homeland Security has an excellent and advanced network of border security tools, but no national system can really compare to a global system. If one were to draw a parallel to cars, one might say that the US has been building the American version of a Ferrari, while Interpol has been building a durable four-by-four. Keeping this simple parallel in mind will be very helpful to recognizing that the needs of the global community are at times different to the needs of any one nation.

National border control systems are necessarily based on internal information and bi-lateral agreements. Unfortunately, bilateral agreements do not offer any guarantees of completeness, and only offer a piecemeal solution to a problem that requires a comprehensive global approach.

By contrast, Interpol has a true and comprehensive system. An automated, global system. A system through which countries feed data directly into the database electronically, and update that data directly and electronically. And it allows border officers worldwide to screen travel documents against that database through connection technology we created, called MIND/FIND.

Unfortunately, wealthy countries sometimes forget that what works for them may not work for other countries. Interpol tries to find global systems that can complement national systems, whether they be advanced or basic. When wealthy countries see the benefits of such a dual, but complementary approach, what was previously thought impossible, becomes possible. The MIND/FIND connections in the Caribbean, for example were possible thanks to financial contributions from Canada.

The US endorsed the use of the SLTD database at border entry points around the world through the US' membership in the G-8, the UN, and ICAO. The world urgently needs this. It is my view that the US and the DHS need to take a leading role in encouraging and assisting countries in making this happen.

## V. Checking Passports Before Passenger Arrival – Placing Additional Tripwires in the Paths of the Terrorists

The airline industry could also play a crucial role in helping to place additional tripwires in the paths of the terrorists – the more time we provide law enforcement between the moment suspicions are raised about an individual's passport and the moment that person shows up at the border, the safer our borders will be. This could be accomplished at a nominal cost and without any inconvenience to travelers. A system could be developed through which, before a plane's departure, the airline sends to Interpol the passport numbers of all the passengers, so that these passport numbers can be cheeked against Interpol's SLTD database, in order to inform relevant law enforcement whether any of the passengers are using any passports that had been reported stolen or lost. The airline would not be transmitting any personal information of the passengers, just the document numbers. If a document number is in the Interpol database, then relevant national law enforcement would be alerted. The control of travel documents in this manner would be non-discriminatory, non-intrusive, and raise no data protection issues. Moreover, since a travel document does not belong to an individual, but is the property of a country, there is no privacy issue with transmitting the document number.

If the travel document had been reported stolen or lost, a hit would be generated and seen by the police in the country that issued the passport, the police in the country from which the passenger is seeking to depart, and the countries to which the individual is travelling. Based on each country's own laws and procedures, the passenger could be detained before departure, so that the hit confirmation process could be conducted and appropriate action taken before departure, or the passenger could be allowed to travel while the hit confirmation process is conducted, and any necessary action could be taken upon arrival at the destination country. Interpol believes that this enhanced security control (which could be financed through a fee-based system) should be encouraged by the US and other countries.

## VI. Conclusion – The World Needs A Truly Global and Comprehensive Border Control System

The recent example of the 11 Iraqis shows that there are organized criminal networks facilitating the illegal international travel of large groups of people. It also shows that US border security does not start in California, Texas, or in the immigration queue at US airports, but in Cyprus, Greece, or Spain. It is in every country's interest to see all the world's border controls strengthened. The organized criminal networks do not care to whom they sell, or for whom they customize stolen passports and travel documents. This problem is clearly global.

With this testimony, Interpol has tried to demonstrate that the gaping hole in global security that terrorists have been exploiting since the first World Trade Center attacks in 1993 might have gotten smaller on a national level, but is still unacceptably large at the global level. Interpol believes that the ability of terrorists to travel around the world based on fraudulent travel documents is the single greatest gap in global security.

Interpol also has tried to demonstrate that any one country's national or bi-lateral approach to border security is destined to fail. Each country works hard to secure its borders. Yet we all too often see, after a terrorist attack, that while the country had been doing a number of things well, there were gaps – gaps that were exploited by the terrorists to deadly effect.

To close this gap, the US and other countries have an interest in seeing that access to the Interpol global SLTD database is implemented, not just in their own country, but worldwide. If deployed throughout the world, we could finally turn towards the root of the problem, by acquiring a global view of the traffic in stolen and lost passports. At this point in time, no single police force in the world has a global overview of the extent of the problem. Widespread implementation of Interpol's MIND/FIND technology could change that and allow us to develop operational and strategic analysis on a global level.

But much more is needed from the entire world community to close this menacing global gap in border security. Let me draw another parallel. Look at the credit card industry and think about the resources that have been dedicated to ensuring that a secure global network is in place to protect the financial interests of the companies and the card holders. Billions of dollars are invested each year to ensure that trillions of dollars of transactions can take place securely. Card holders and criminals alike know that within minutes of reporting a credit card as stolen, the card's use can be canceled worldwide. It is not enough that the credit card is canceled in one country; it must be canceled in all countries for the issuing card company and for the card holder to be safe. The system works so well and so much is invested in maintaining the system that even unusual purchase patterns can be identified in time to permit instant verification that you are the legitimate cardholder. Why? To protect the financial interests and very existence of the card issuer, as well as to ensure that the global economy can function properly and continue to grow.

Now, take a look at passports. How many resources have been dedicated to ensure that the most precious and valuable national identity document (the passport) remains secure nationally and globally? How many citizens diligently stand in line removing their shoes, belts, clothing, baby formula, toothpaste and any other "suspicious" item because their governments tell them it is in their security interest to do so? What would these same citizens think if they knew that when they or others handed their passports at points of entry, these passports were not being screened against the world's only global database containing nearly 7 million stolen passports? They would be shocked. I know the answer to this question because I have traveled to over 100 countries as Interpol Secretary General, making this and other points about the urgent need to check global databases to ensure national security.

The question that keeps me up at night is this. If a terrorist attack occurs, and the terrorists used stolen travel documents, but those travel documents were not screened against Interpol's Global Stolen and Lost Travel Document database, what would we tell loved ones of those who were murdered? Could tell them that we did everything in our power to prevent it? Could we say that we were not aware of the risk? Could we say that we had other more important priorities? Could we say that we did not have a billion dollars to invest annually as a global community?

Let me close with the parallel that I used earlier because I do not want to be accused of using fear tactics to dramatize my point.

Let's continue to encourage countries to build Ferraris, for they serve a very useful purpose if you want to get somewhere really fast and you know the kind of road conditions that you will encounter. But, let's remember that if you did not know where you had to go really fast and if you did not know what road conditions you would encounter, would you pick a Ferrari or a four-by-four as your vehicle of choice?

In this epic anti-terrorist struggle in which we find ourselves, where terrorists and other dangerous criminals are trying to kill our citizens – often indiscriminately, we do not have the luxury of knowing where or under what conditions, we will encounter them. So, it is my firmly-held belief that we had better invest in building a dual, yet complementary, national and global border security system.

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

# Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents

**Testimony of**

**Andrew Simkin**

**Director, Office of Fraud Prevention Programs**
**Bureau of Consular Affairs**
**U.S. Department of State**

**May 2, 2007**
**10:00 a.m.**

---

Chairman Feinstein, Ranking Member Kyl, distinguished members of the Subcommittee:

I appreciate this opportunity to discuss the efforts of the Department of State's Bureau of Consular Affairs (CA) to interrupt terrorist travel. The Department has responsibility for the proper adjudication of passport and visa applications in accordance with U.S. law. Consular officers interview foreign nationals and individuals with claims to U.S. citizenship at over 200 Foreign Service posts around the globe. This is the front line – the first and probably the best opportunity to detect deception and prevent a terrorist or other criminal from traveling to our country.

## Secure Travel Documents

The 9/11 Commission noted that travel documents are as valuable as weapons to terrorists. Altered passports and visas, or genuine documents obtained fraudulently, allow terrorists – and other criminals – to cross borders in the course of planning or carrying out operations.

U.S. passports and visas are among the most valuable and highly sought-after travel documents in the world. Demand for them is high, and rising. The Department issued 12.1 million U.S. passports in FY 2006, an all-time record. We anticipate issuing more than 17 million this year. We issued 5.8 million nonimmigrant visas in FY 2006 – 8.3 percent more than in 2005 – while refusing visas to 1.9 million visa applicants.

The Department is committed to ensuring that U.S. citizens have passports when they need to travel and to providing transparent, efficient visa adjudication for legitimate tourists, business visitors, students, and other travelers, whose visits to the United States we encourage and value. At the same time, we will not compromise our commitment to the security of such documents and the integrity of the consular adjudication processes.

Passports

On August 14, 2006, at our Colorado Passport Agency, the Department of State began issuing to the public a redesigned U.S. passport that for the first time includes facial recognition biometrics and a contactless chip embedded in the book. These "e-passports" are the most secure U.S. passport ever produced and represent a major enhancement in ensuring the integrity of travel documents.

We adopted a multi-layered approach in designing the e-passport in order to implement higher security standards, address privacy concerns, and protect personal data. The result is a document that is considerably more difficult to counterfeit or for an impostor to use should it be lost or stolen.

A digitized photo of the bearer on the data page is the standard passport biometric adopted by the International Civil Aviation Association (ICAO). A radio frequency identification (RFID) microchip embedded in the back cover contains the same identifying information printed on the data page of the passport – name, date of birth, gender, place of birth, dates of passport issuance and expiration, passport number, and the digitized photo image of the bearer. The data written to the chip is protected from alteration by the use of a Public Key Infrastructure (PKI) digital signature.

The e-passport incorporates other overlapping security measures to protect the bearer's privacy and secure personal data. Metallic webbing in the front

cover and spine of the book prevents surreptitious "skimming" of the data on the chip while the book is closed. This is complemented by Basic Access Control (BAC) technology, which requires that the passport's machine-readable zone be read in order to generate the electronic key that unlocks the chip. To address the concern that the RFID chip might be used to track the bearer, we employed Randomized Unique Chip Identifiers (RUIDs), which generate a different ID number each time the chip is read by a passport chip reader.

With traditional passports, two things must match in a legitimate case: the face of the bearer and the data on the photo page. Detection of photo substitution or other tampering is dependent upon the border inspector's training and expertise. With the e-passport, three things must match to confirm that the traveler is the person to whom the passport was issued: the face of the traveler, the data on the photo page, and the data on the chip. The immigration inspector scans the passport and, in a matter of seconds, will be able to confirm the identity of the passport bearer. Border authorities can better intercept suspect travelers and speed entry of legitimate travelers. Further, border authorities in other countries can in effect assist us in managing the integrity of e-passports each time they report instances when the three elements don't match.

In developing the e-passport, we consulted frequently with industry experts and solicited public comments through the Federal Register before beginning production. We conducted rigorous tests of the chip's security with technical experts from the private sector and the National Institute of Standards and Technology to assess the risk of unauthorized reading and to evaluate the efficacy of countermeasures. We are confident that unauthorized individuals will not be able to extract information from the chips.

To date, we have issued three million U.S. e-passports. All of our domestic passport agencies and one passport center have been fully converted to issue e-passports. Conversion of the one remaining passport center should be completed later this month.

When reviewing our passport operations, we identified emergency passports – those issued by posts overseas to replace lost or stolen passports for U.S. citizens – as a potential vulnerability in the passport security program

because such passports used glued or laminated photos of the bearer, which are easier to substitute or alter than digitized photos. We have replaced the old passports with a more secure photo-digitized passport. We launched the Emergency Photo-Digitized Passport (EPDP) in fall 2006. Since February 2007, U.S. embassies and consulates issue only the EPDP in emergency cases.

The data for an EPDP are printed on a secure foil – similar to that used for U.S. visas – which is then sealed to a page by a heat laminate that is difficult to alter without destroying the laminate or data page. Digital security fields incorporated into the foil encode data viewable only with a special lens or decoding software. An additional data coding scheme indicates tampering if the data page is modified.

I would be happy to share with the Subcommittee samples of the e-passport and the EPDP.

In anticipation of the implementation of the land border phase of the Western Hemisphere Travel Initiative (WHTI), and to meet the unique needs of the border community, the Department is also developing, in coordination with the Department of Homeland Security (DHS), a limited-use passport card as a secure alternative document to the traditional passport book.

The convenient wallet-sized card will contain a vicinity-read RFID electronic chip to meet the operational needs at DHS ports of entry (POEs). State-of-the-art security features will be used to reduce the risk of counterfeiting or forgery. The chip will contain a unique identifier number rather than sensitive personal data. The number will be linked to a secure database maintained by the Departments of Homeland Security and State.

We are aware that vicinity-read RFID technology has raised concerns about data privacy, and we are working actively with industry to address those concerns. We are committed to providing a durable and highly secure passport card to the American public.

Visas

The Department has incorporated biometric technology – specifically, facial recognition and fingerprint scans – into U.S. visa processes as well. The U.S. BioVisa program is completely integrated with the DHS US-VISIT program, so that anyone entering the United States on a nonimmigrant visa can be identified through biometrics.

All visa applicants submit a photo with the application. A digitized image of the photo is included on the visa, as well as in the electronic visa record.

In September 2003, we began deploying fingerprint scanners to overseas posts, and by October 2004, all posts were collecting electronic fingerprints, thus meeting the statutory deadline established by the Enhanced Border Security and Visa Entry Reform Act of 2002. We collect two fingerprints from each visa applicant (other than for diplomats and those under the age of 14 or over 79). Prior to visa issuance, the fingerprints are cleared against the DHS Automated Biometric Identification System (IDENT), which contains fingerprints of known or suspected terrorists (KSTs) and of persons wanted by law enforcement. We have cleared fingerprints of over 17 million visa applicants through IDENT. Over 35,000 IDENT matches have been investigated by consular officers and, where appropriate, have resulted in visa denials. More recently, we have successfully completed a pilot test of a new process for electronically collecting 10 fingerprints, rather than two. Ten fingerprints provide a greater number of data points, allowing more complete checks against criminal history fingerprint records and much more accurate responses. We have begun rolling out this technology to posts, and we expect to complete worldwide deployment by the end of 2007.

**Passport and Visa Adjudication Processes**

Even more important than the security of documents themselves is the integrity of the adjudication process, including the electronic databases used to screen applicants and verify their status. All valid U.S. passports are supported by PIERS, a database of passport records, including photos, applications, and history, which is available to consular officers and passport adjudicators worldwide to verify the identity and citizenship of those to whom U.S. passports have previously been issued.

The Consular Lost and Stolen Passports (CLASP) database includes over 1.3 million records concerning U.S. passports. All passport applications are checked against CLASP, PIERS, the Social Security Administration's database, and the Consular Lookout and Support System (CLASS), which includes information provided by the Department of Health and Human Services (HHS) and law enforcement agencies such as the Federal Bureau of Investigations (FBI) and U.S. Marshals Service.

Every visa applicant also undergoes extensive security checks before a visa can be issued. Our system automatically runs a name-based check in a database that currently includes more than 20 million entries. These entries include State Department information, FBI files, immigration violations, and intelligence from other agencies. All visa applications are checked against derogatory information of KSTs in the Terrorist Screening Database (TSDB). The TSDB integrates terrorist watchlists from all U.S. Government (USG) sources. It is maintained by the Terrorist Screening Center (TSC), which serves as the centralized point of contact for hits against the watchlists. Hits are reviewed by USG agencies in Washington, D.C., prior to any visa being approved. New KST entries are checked against records of previously issued valid visas, enabling us to prudentially revoke those visas. Since 9/11, we have revoked more than 1,700 visas of individuals suspected of being connected to terrorism.

Our consular lookout database contains information from past findings of visa ineligibility as well as information from other agencies. When a consular officer determines that an applicant matches a "hit" in the database, or if the applicant meets other established criteria, the case is referred for an interagency security review in Washington, D.C., resulting in a Security Advisory Opinion (SAO) sent back to the consular officer. We processed nearly 245,000 SAOs in FY 2006, and over one million since 9/11.

**The Consular Visa Interview**

One of the most significant changes in consular practice after September 11 was a re-emphasis on the personal interview. The interview is the best available tool for detecting an applicant who has criminal intentions but whose name, fingerprints, and photo do not match any derogatory information previously known to the U.S. Government.

In these interactions, the consular officer has an inherent advantage in that the mala fide applicant, in preparing a cover story for his mala fide travel, cannot possibly plan and memorize answers to all of the infinite variety of questions that the consular officer may ask. Furthermore, per section 291 of the Immigration and Nationality Act, the burden of proof is on the visa applicant. Per section 214(b) of that Act, if the applicant does not establish his eligibility for a visa to the satisfaction of the consular officer, then the visa must be denied.

Making these decisions demands every bit of preparation that the consular officer can bring to bear in terms of intellect, foreign language skill, human understanding, cultural awareness, and judgment. We cannot guarantee that every terrorist will be detected and denied by an alert consular officer. However, the array of measures we have put in place, including analytic interviewing techniques, biometric checks, database checks, and document verification, poses a significant obstacle and deterrent to persons seeking entry to the United States to do us harm.

**Other Fraud Prevention Techniques**

We have a variety of tools available, in addition to the consular interview, to separate fact from fiction in visa applications. Consular Fraud Prevention Managers and locally-engaged staff conduct field inquiries, visit Civil Registries, telephone employers or schools, and consult local contacts. We employ increasingly sophisticated electronic search capabilities to detect links between different fraudulent cases or to check an applicant's story against available sources of data. Consular officers often consult Internet resources including maps and satellite photos to verify the information contained in visa applications.

Our principal goal in these endeavors is to reach the right decision regarding the visa or passport application. Often, however, we run across organized or egregious fraud that may be prosecutable in the United States or under local law. In such instances we turn immediately to our law enforcement colleagues in the Bureau of Diplomatic Security (DS). CA and DS coordinate very closely. Many DS agents go through the basic consular course and may be assigned as overseas criminal investigators based in the consular section at a Foreign Service post. In many cases, based on DS's excellent liaison relationships with local police, a perpetrator of fraud not

only is rejected for a visa, but is then placed under arrest at the front gate on departing the Embassy. I believe that this coordination with DS is a very powerful factor in deterring terrorist attempts to secure visas, as well as deterring other kinds of fraud.

CA and DS have established a jointly-staffed Vulnerability Assessment Unit (VAU) within CA's Office of Fraud Prevention Programs. The VAU is responsible for strengthening internal controls and investigating cases of internal corruption or malfeasance, for which we adhere strictly to a policy of zero tolerance.

CA also works with Immigration and Customs Enforcement Visa Security Unit (ICE/VSU) officers who are assigned overseas as mandated by section 428 of the Homeland Security Act of 2002. Visa Security Units are required to review 100 percent of visa applications in Saudi Arabia. CA is working cooperatively with ICE/VSU as they consider expanding to additional posts.

**Enhanced Training for Consular Officers**

Given the key point of control that consular officers occupy in screening U.S. travel documents, the Bureau of Consular Affairs accords the highest priority to providing comprehensive training to consular officers. Working with the Department of State's Foreign Service Institute, we have expanded and updated basic and continuing training programs for consular officers, with a particular focus on anti-fraud measures.

There are currently more than 1,600 consular officer positions. The Department of State created 570 of these since 9/11 to increase the resources dedicated to consular adjudication.

Every officer assigned to serve a consular tour must first complete the 31-day Basic Consular Course, and any officer returning to consular work after performing non-consular work for five years or more is required to repeat the course. In addition to covering the core consular subjects of passports, visas, American citizen services, consular interviewing, and consular management, the course has been enhanced to include lessons learned from 9/11. It includes briefings and hands-on analysis of documents to help students practice recognizing the security features of genuine travel documents and indicators of altered and counterfeit documents. Trainees

also learn to detect impostors who may present genuine documents not legitimately belonging to them. Since 2003, the course has included training in interview techniques designed to spot inconsistencies in an applicant's story or demeanor and the micro facial inflections applicants may betray when experiencing emotions during the interview.

Additional training courses beyond the Basic Consular Course keep consular officers current and enhance their ability to detect, intercept, and disrupt terrorist travel. In conjunction with FSI, we have accomplished the following:

- Created a new course, Advanced Consular Namechecking, to provide visa officers a detailed understanding of the results from the various lookout systems (including namechecks, biometrics, and facial recognition). Since 2002, when the course was first introduced, 709 consular officers have attended this four-day course, and an additional 107 officers have attended a one-day version offered overseas.

- Established a new one-day course on Consular Interviewing to ensure that mid-level consular managers have access to new content on detecting deception which was added to the Basic Consular Course. To date, 625 consular officers and passport examiners have taken this course.

- Expanded offerings of the five-day Fraud Prevention for Consular Managers course from two to eight per year, increasing enrollments from 42 in FY 2004 to 185 in FY 2006. The course curriculum includes a briefing on terrorist travel, hands-on training in use of classified SIPRnet resources and unclassified USG and commercial databases, briefings from DHS, and instruction on document analysis.

- Launched distance learning courses on Detecting Impostors, Detecting Fraudulent Documents, and Examining U.S. Passports. Consular personnel all over the world, as well as other personnel such as diplomatic security special agents and other agency officials can now access these courses from their desktops.

- Sponsored regional fraud prevention conferences for consular officers assigned to the Middle East, the Western Hemisphere, East Asia,

Europe, and Africa. Fraud prevention training has also been incorporated into nine regional Consular Leadership Development Conferences (CLDCs) during FY 2006 and FY 2007.

In addition to formal fraud training provided to officers and locally employed staff, CA's Office of Fraud Prevention Programs assists posts in continuously improving fraud prevention and detection techniques by analyzing and sharing fraud information, providing consular officers with access to advanced databases and other technological tools, and liaising with other agencies.

**Information Sharing**

Developing secure travel documents and training our staff are important tools in disrupting terrorist travel. As the 9/11 Commission noted, this effort also requires collaboration with other nations. The Department recognizes that routine and timely information sharing within the USG, with international organizations, and with other governments is critical to success, and we are pursuing this aggressively on a number of fronts.

Interagency Datashare

CLASS continues to operate its well-tuned, two-way sharing of lookout names with the DHS Treasury Enforcement Communications System (TECS), which is used at ports of entry. The overall CLASS database of names has risen to over 20 million records in recent years, including millions of names of criminals from FBI records provided to the State Department under the terms of the USA PATRIOT Act.

Up to 35,000 files on issued visas are transferred daily to TECS within minutes of issuance at posts around the world, while fingerprints collected with these visas are transferred to the DHS IDENT fingerprint system.

In addition to sending data to TECS and IDENT, CA has actively shared with other agencies access to its consular consolidated database (CCD). Over 8,000 users from DS, DHS, FBI, the Departments of Commerce, Defense, and Justice, and other U.S. Government agencies have access to the CCD, making over one million queries per month.

Datashare with International Organizations

In 2004, the Department began transferring data on U.S. lost and stolen passports to Interpol. We have shared all the data we have – more than 1.3 million records. The United States is the largest single contributor of lost and stolen passport data to Interpol's Automated Search Facility/Stolen and Lost Travel Document Database (ASF/SLTD). This database contains more than 14 million recorded lost/stolen documents.

Access to records in the Interpol system is not automatic or in real time. An immigration or border official must suspect the authenticity of a traveler's documentation and in each case query the Interpol database. The Department recognizes the need to establish a systematic and routine mechanism for widespread use of the Interpol database at U.S. Foreign Service posts and POEs. The primary challenge is developing access architecture that would support the volume of queries involved and the ability to get responses in real or near-real time.

Information Sharing with Other Governments

Another vital aspect of disrupting terrorist travel involves international sharing of information on terrorists. Within the Department of State, the Bureau of Consular Affairs has the lead on negotiating with foreign governments for the international sharing of terrorist lookout information, under authority delegated pursuant to Homeland Security Presidential Directive Number 6 (HSPD-6). The United States has pre-existing agreements that satisfy the requirements of HSPD-6 with Australia and Canada. We have approached all 27 countries currently participating in the Visa Waiver Program, as well as a limited number of other key partners.

We have signed HSPD-6 agreements with three countries and are finalizing the technical details for beginning the data exchanges. We are engaged in working level discussions with 10 countries and have received serious expressions of interest from six others. The goal of these arrangements is to ensure the timely receipt of information on KSTs before they travel, so that consular officers, POE inspectors, and others can make informed, accurate, timely decisions and disrupt the travel of potential terrorists.

**Conclusion**

Madam Chairwoman, we are focused on maintaining the security of U.S. travel documents, while optimizing the technology, procedures, information, and training that go into the issuance and verification of travel documents. Consular officers occupy the front line in interrupting terrorist travel. At the same time, we may be the first American officials that millions of legitimate travelers meet. The impression that we make may well form a lasting opinion of America in their minds. We are thus responsible for securing our country and for serving as its public face. It is an honor to carry these responsibilities, and we will continue to do so to the very best of our abilities.

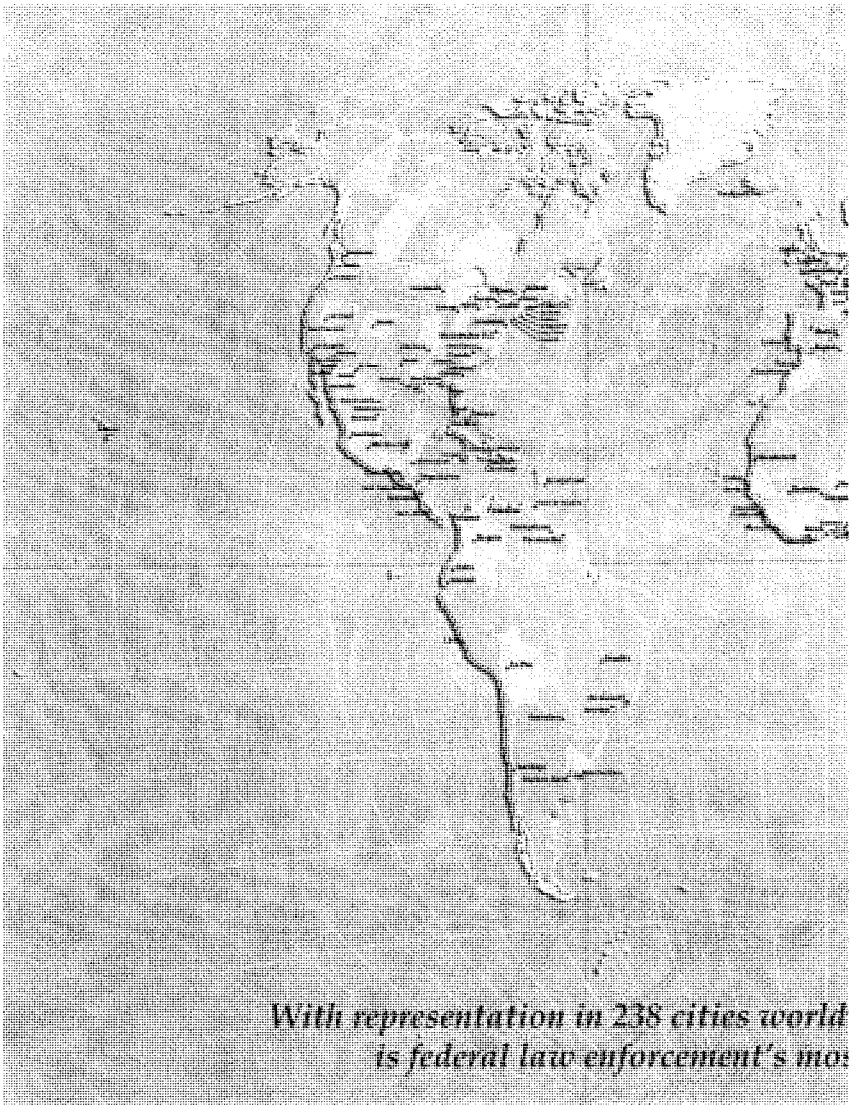
# VISA AND PASSPORT SECURITY STRATEGIC PLAN

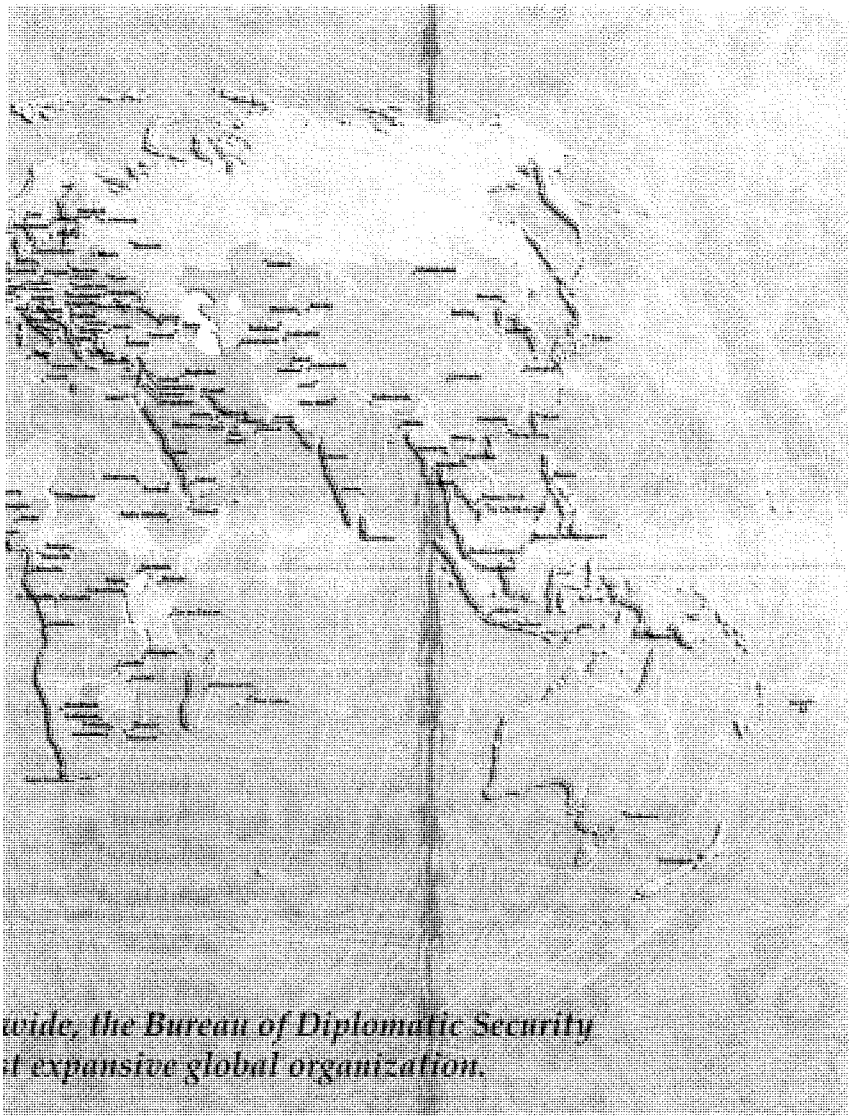
*United States*

*Department of State*

## Mission Statement

The Bureau of Diplomatic Security is dedicated to the U.S. Department of State's vision to create a more secure, democratic, and prosperous world for the benefit of the American people and the international community. To meet the challenge of safely advancing and protecting American interests and foreign policy, the Bureau of Diplomatic Security's global law enforcement mission protects the U.S. Secretary of State; secures American diplomatic missions and personnel; and upholds the integrity of U.S. visa and passport travel documents.


With representation in 238 cities world
is federal law enforcement's mo



*wide, the Bureau of Diplomatic Security*
*it expansive global organization.*

## Table of Contents

Map of DS Worldwide Locations . . . . . inset

Mission Statement . . . . . inset

Introductory Letter from Assistant Secretary Griffin . . . . 3

The Bureau of Diplomatic Security: A Brief History . . . . . 5

Visa and Passport Fraud: An Overview . . . . . 7

Introduction . . . . . 9

Strategic Goal 1 . . . . . 13

Strategic Goal 2 . . . . . 19

Strategic Goal 3 . . . . . 25

Conclusion . . . . . 29

Appendix: Operation Triple X . . . . . 31

*Except where noted, all images U.S. Department of State*

VISA AND PASSPORT SECURITY STRATEGIC PLAN

2

December 5, 2006

In accordance with the requirements of Section 7218 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), I am pleased to submit the Visa and Passport Security Strategic Plan of the Bureau of Diplomatic Security (DS).

As the law enforcement entity in the Department of State, the Bureau of Diplomatic Security upholds the integrity of U.S. visa and passport documents through the enforcement of Chapter 75 (Passports and Visas) of the U.S. Criminal Code, including our visa and passport fraud statutes. The Special Agents of the Bureau of Diplomatic Security conduct criminal investigations into passport and visa violations throughout the Department's foreign diplomatic missions and domestic issuance facilities. Overseas, DS Special Agents work with our foreign partner nations to target and disrupt document fraud rings and human smuggling networks. In the homeland, our agents work with local, state, and federal law enforcement agencies to investigate, arrest, and prosecute document fraud violators. Through this global network of law enforcement professionals, DS Special Agents are on the frontlines of combating terrorist travel.

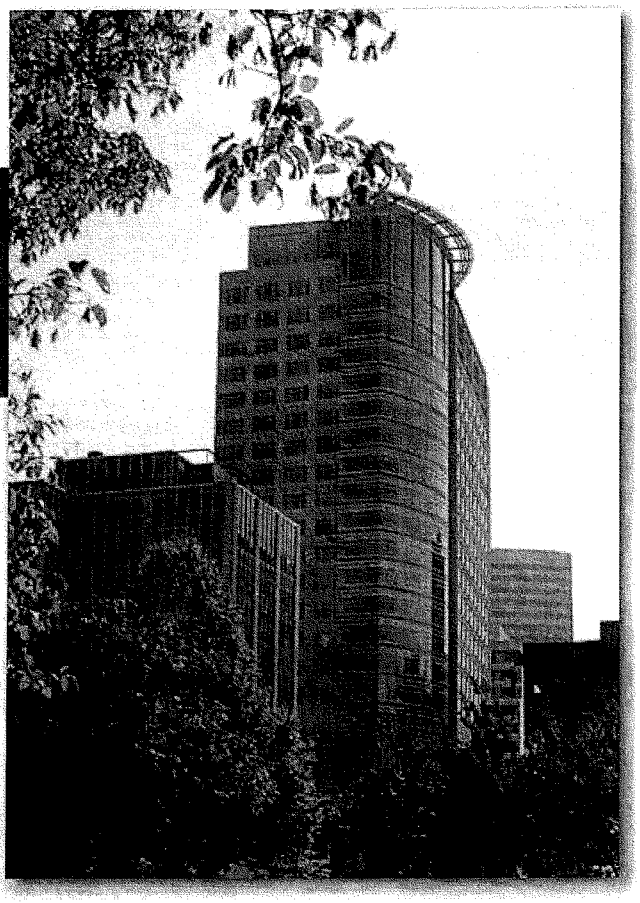
To illustrate the magnitude of the fraudulent travel document challenge that must be confronted to protect the homeland, I would like to draw your attention to DS's investigative efforts in Surabaya, Indonesia. Over the past two years, the DS Regional Security Office in Surabaya has solicited the cooperation of Indonesian law enforcement authorities to curb the availability of illegally obtained and counterfeit identification documents. The ensuing joint DS and Indonesian operation resulted in 20 police raids in Surabaya and Bali. These raids generated 84 arrests, 6 fugitive extraditions to the United States, and shut down 20 vendors of fraudulent documents. Criminal charges filed include such violations as human trafficking, prostitution, child pornography, and pedophilia. It is estimated that these vendors were used by more than 8,000 individuals seeking fraudulent documentation. Most disturbing was the discovery that these document rings were used by members of the Indonesian terrorist group, Jamal Islamyia, to obtain counterfeit identification documents. Included in the appendix of the Plan is a case overview of Operation Triple X, detailing the successes of DS's investigative efforts and partnership with Indonesian law enforcement.

The Surabaya case, Operation Triple X, is but one example of individuals and groups around the world that seek to manipulate and exploit vulnerabilities within the travel document system. As federal law enforcement's most expansive global organization, DS is uniquely positioned and committed to meet this challenge. To achieve success, DS has crafted a Strategic Plan that leverages our international expertise and presence and focuses on the key components of aggressive enforcement action, coordinated intelligence efforts, and foreign capacity building. This strategy provides the framework for a worldwide Visa and Passport Security Program and will augment significantly the Department's efforts to identify, disrupt, and target terrorist travel.

Implementation of the Department's Visa and Passport Security Program will be dependent upon significant new resources and the global deployment of additional DS Special Agents, intelligence analysts, Foreign Service national investigators, and support staff. Within three years, DS will have dedicated Special Agents combating terrorist travel, document fraud, and human smuggling and trafficking at 200 overseas posts. I am committed to fulfilling the strategy's vision and look forward to working with Congress to obtain the personnel and resources essential for the Program's success.

Sincerely,

Richard J. Griffin
Assistant Secretary
Bureau of Diplomatic Security



# The Bureau of Diplomatic Security: A Brief History

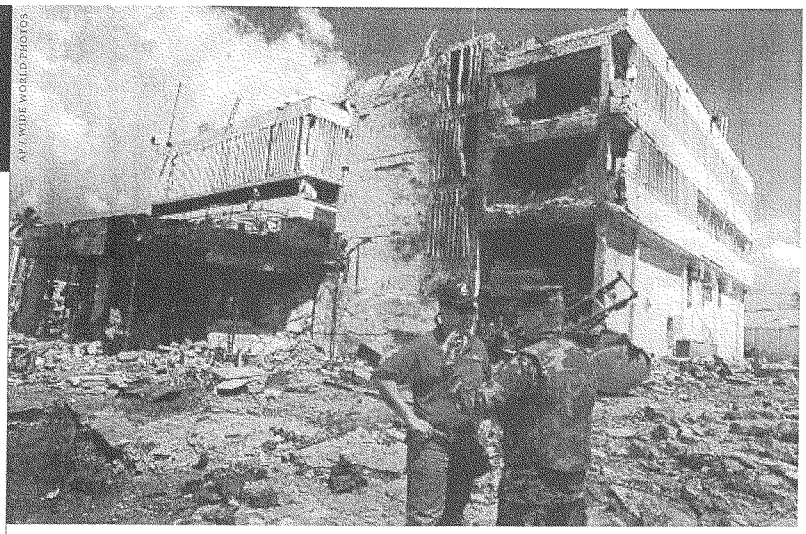
The Bureau of Diplomatic Security is the security and law enforcement arm of the U.S. Department of State. Throughout its 90-year history, DS has contributed significantly to the Department's mission and to the national security of the United States.

## HISTORICAL VISA AND PASSPORT INVESTIGATIVE FUNCTION

Security within the U.S. Department of State was established formally in 1916 under U.S. Secretary of State Robert Lansing. At that time, the Chief Special Agent also carried the title Special Assistant to the Secretary and reported directly to the Secretary of State on special matters. A handful of agents worked out of Washington, D.C. and New York City and conducted a wide range of sensitive investigations, with a special focus on the operations of foreign agents and their activities in the United States.

DS's authorities pertaining to travel documents were established in 1918, when Congress passed legislation requiring passports for Americans traveling abroad and visas for foreign nationals seeking to enter the United States. Soon thereafter, the Department of State's Chief Special Agent's Office—DS's predecessor—began investigating passport and visa fraud. Ensuring the integrity of the U.S. passport and visa has remained a core responsibility, even as DS's mission continues to evolve to meet the changing security needs of the State Department.

In 1984, in the aftermath of the Beirut terrorist bombings, U.S. Secretary of State George Shultz formed an advisory panel to study the increasing problem of terrorist attacks on U.S. diplomats and facilities overseas. Chaired by retired U.S. Navy Admiral Bobby Inman, the Advisory Panel on Overseas Security (Inman Panel) conducted an exhaustive examination of the Department's security programs. In June 1985, the Inman Panel submitted its recommendations to the Secretary of State, which resulted in the creation of the Bureau of Diplomatic Security and the Diplomatic Security Service. The Inman Panel's recommendations also encompassed ensuring the integrity of U.S. visas and passports. The recommendations were codified by Congress with passage of the Omnibus Diplomatic Security and Antiterrorism Act, which was signed into law by President Reagan on August 27, 1986.



AP/WIDE WORLD PHOTOS

## AN ESTABLISHED AND UNIQUE GLOBAL PRESENCE

The tragic 1998 bombings of U.S. embassies in East Africa served as a catalyst to enhance DS's responsibilities for ensuring the security of State Department personnel and facilities. DS partnered with the Bureau of Overseas Buildings Operations to establish blast-resistant, yet aesthetically pleasing, office space worldwide. That partnership has resulted in more than 50 new embassy compounds and design innovations that make possible the building of facilities in challenging environments, such as construction of the new embassy compound in Baghdad.

Another outcome of the 1998 East Africa bombings was the expansion of DS's federal law enforcement efforts, engendering a truly global presence and impact. In addition to DS's 25 field and resident offices in the United States, one-third of DS Special Agents are assigned to U.S. embassies and consulates in 159 foreign nations, providing security for 269 U.S. diplomatic posts. No other federal law enforcement agency can boast such a geographically diverse presence in the international law enforcement community. This has allowed DS to forge working relationships with foreign police, security services, and international law enforcement organizations worldwide. In the post-9/11 world, DS's ability to coordinate a myriad of foreign and U.S. local, state, and federal law enforcement agencies to protect U.S. interests is both unparalleled and critical. DS can identify and facilitate the arrests and prosecutions of potential terrorist suspects through this global network before they even reach American shores.

# VISA AND PASSPORT FRAUD: AN OVERVIEW

## THE 9/11 COMMISSION REPORT

*"For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. Because they must pass through regulated channels—presenting themselves to border security officials—or attempt to circumvent inspection points, international travel poses great danger to terrorists. In their travels, terrorists use evasive methods, such as altered and counterfeit visas and passports, surreptitious travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud."*

The borders of the United States are at risk every day from individuals who attempt to secure valid U.S. visas or passports by illegal means. The Department's consular officers are challenged constantly in their efforts to identify potential irregularities in visa applications, false documents, and a host of other deceptions that individuals employ to obtain a U.S. visa by fraudulent means. The difficulty of this mission is compounded by the sheer number of valid applications and by the location of U.S. consular facilities overseas. In many locations, applicants have unlimited access to fraudulent documents and/or corrupt officials who illegally provide apparently legitimate travel documents. Many of these applicants will spend their life savings to obtain fraudulent travel documents or the services of smuggling networks even if they are given no guarantee of success. The U.S. passport is in even greater demand. The most valuable travel document in the world, it establishes U.S. citizenship and allows its bearer unlimited access to the United States and many other countries.

# Visas Departures/Sorties

Counterfeiting of visas and passports is at the core of a wide range of threats posed by terrorists and transnational criminal organizations. DS's partnership with the State Department's Bureau of Consular Affairs (CA) is essential for DS to investigate and enforce violations of visa and passport criminal statutes in both the United States and overseas. DS criminal investigations have uncovered a wide range of illicit travel facilitation crimes, including:

- ★ *Terrorists who use counterfeit, criminally acquired, or altered travel documents;*
- ★ *Narcotics traffickers and others who attempt to acquire U.S. passports under false names to avoid detection by law enforcement;*
- ★ *Fugitives from justice who use aliases to obtain U.S. passports;*
- ★ *Individuals and groups that supply travel and supporting documents to criminals, human smuggling and trafficking organizations, and identity theft and financial fraud rings;*
- ★ *Visa applicants who use fraud in an attempt to visit, work, or reside illegally in the United States.*

The 9/11 terrorists succeeded in carrying out their attacks through the use of fraudulently obtained, but genuine, U.S. travel documents. Throughout the 1990s, members of al-Qaeda learned to exploit weaknesses in the immigration, passport, visa, and entry systems of the United States. They successfully instituted a travel facilitation operation in Afghanistan through the use of travel agents, document forgers, and corrupt government officials. The 19 hijackers employed a variety of methods to conceal their identities, including the use of 364 aliases, fraudulent entry-exit stamps, and altered passports. Through these fraudulent methods, the 9/11 terrorists obtained legitimate passports and tourist visas, entered the United States, and perpetrated the largest terrorist attack in our nation's history.

*(Source: 9/11 and Terrorist Travel. Staff Report of the National Commission on Terrorist Attacks Upon the United States).*

## INTRODUCTION

In December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) to implement the recommendations of the 9/11 Commission. The 9/11 Commission had identified a number of factors that allowed terrorists to exploit the vulnerabilities of U.S. travel documents. The IRTPA directed the National Counterterrorism Center (NCTC) to develop a National Strategy to Combat Terrorist Travel (NSCTT). That strategy, which was submitted in March 2006, enhances the capabilities of the United States and its foreign partners to "constrain terrorist mobility overseas" and "deny terrorists the ability to enter, exit, and travel within the United States." The President's updated "National Strategy for Combating Terrorism," issued in September 2006, builds upon the NSCTT and reinforces the twofold need to "deny terrorists entry to the United States and disrupt their travel internationally" and "strengthen coalitions and partnerships."

In anticipation of the NSCTT, Section 7128 of the IRTPA mandated the establishment of a Visa and Passport Security Program (Program) within the Department of State's Bureau of Diplomatic Security to safeguard the integrity of U.S. travel documents. The Program is required to target and disrupt terrorist travel and includes the following four components: Analysis of Methods; Identification of Individuals and Documents; Identification of Foreign Countries Needing Assistance; and Inspection of Applications.

In establishing this Program, Section 7218 required that DS:

> *... shall ensure the preparation of a Strategic Plan to target and disrupt individuals and organizations, within the United States and in foreign countries that are involved in the fraudulent production, distribution, use, or other similar activity—*
>
> *(A) of a United States visa or United States passport;*
>
> *(B) of documents intended to help fraudulently procure a United States visa or United States passport, or other documents intended to gain unlawful entry into the United States; or*
>
> *(C) of visas and passports issued by foreign countries intended to gain unlawful entry into the United States.*

The DS Strategic Plan (Plan) incorporates the principles of the NSCTT and the President's overarching national strategy and addresses the IRTPA's objective to target and disrupt individuals and organizations that attempt to compromise the integrity of U.S. travel documents. Successful implementation of the strategy will diminish terrorists' opportunities to operate and recruit; restrict access to potential U.S. targets; and allow U.S. domestic agencies to concentrate more of their resources on critical infrastructure, border security, and immigration policy. The Plan will require the deployment of additional DS personnel at critical posts around the globe, resources to enhance intelligence and data-sharing efforts, and vital training and technical assistance to our foreign partners.

The Plan is built upon three strategic goals:

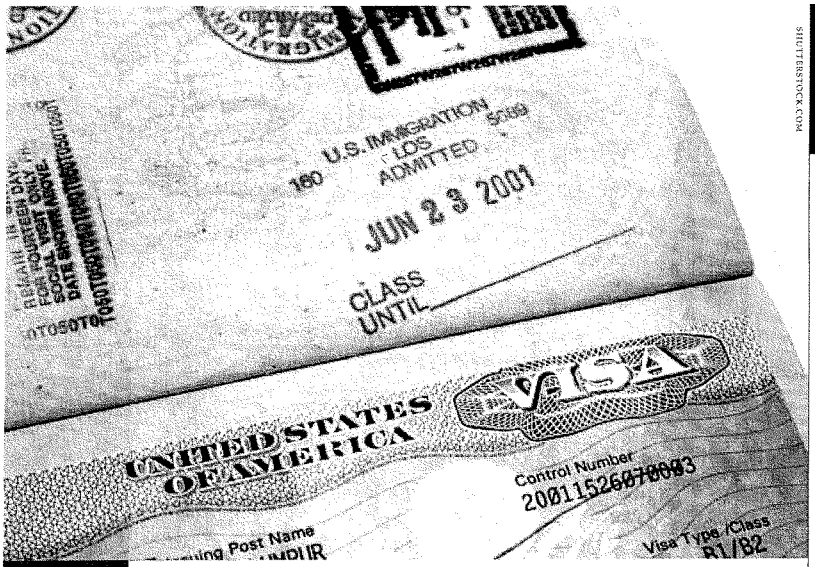
***Strategic Goal 1***
***Defend the homeland and our foreign partners from terrorist attack through aggressive and coordinated international law enforcement action.***

***Strategic Goal 2***
***Detect terrorist activity, methods, and trends that exploit international travel vulnerabilities.***

***Strategic Goal 3***
***Disrupt terrorist efforts to use fraudulent travel documents through strengthening the capacities of foreign partners.***

Achieving these three strategic goals will require the creation of a robust global force capable of combating terrorist travel and attempts to obtain U.S. visas and passports by illegal means. The Plan emphasizes law enforcement efforts and coordination; interagency collaboration, information exchange, and intelligence analysis; and foreign cooperation and capacity building.

The success of the Plan will be a direct result of collaboration with bureaus within the State Department. The databases and expertise of the Bureau of Consular Affairs are critical to identifying and disrupting terrorist travel. The Department can leverage additional expertise in identification and analysis of suspicious patterns, symbols, or associations from the NCTC and the Human Smuggling and Trafficking Center (HSTC) and dedicate resources appropriately. Such analysis will assist border screeners, ease impediments to legitimate travel, and stop terrorists before they ever reach U.S. shores.




SHUTTERSTOCK.COM

DS also works closely with the Secretary's Counterterrorism Coordinator and the Bureau of International Narcotics and Law Enforcement in their missions to enhance the counterterrorism capacity of foreign governments. This Plan builds upon existing cooperative relationships and outlines expanded efforts to provide training through the International Law Enforcement Academies. By developing local expertise and regional cooperation, the Plan will increase dramatically the ability of the United States and its partners to inhibit terrorists' mobility.

DS and the security entities that preceded it at the State Department have conducted passport and visa fraud investigations since 1918. The men and women who join DS do so because they want to serve the federal law enforcement community in overseas locations. DS personnel receive rigorous and specialized law enforcement, intelligence, and language training to ensure they are properly prepared to perform their duties at State Department posts throughout the world. DS's unique combination of foreign and domestic partners will facilitate the effective implementation of this Strategic Plan.

US
DEPARTMENT OF STATE
DIPLOMATIC SECURITY SERVICE
SPECIAL AGENT

## STRATEGIC GOAL 1

*Defend the homeland and our foreign partners from terrorist attack through aggressive and coordinated international law enforcement action.*

Investigating and targeting criminals who generate and/or use fraudulent travel documents is the most effective means by which to disrupt terrorist mobility, human smuggling, and human trafficking. Such investigations require a coordinated international and domestic law enforcement effort to ensure that terrorists and criminal violators are investigated, arrested, and prosecuted wherever these transgressions occur. DS is uniquely positioned to accomplish this increasingly important dimension of U.S. counterterrorism activities and crime prevention.

Overseas, DS created a pilot project that assigned Special Agents to investigate visa and passport fraud at posts where high levels of fraudulent travel documents had been detected. These agents work with their host countries' law enforcement authorities to combat the production of fraudulent travel documents in order to disrupt terrorist travel. Since the pilot project's inception in 2004, the results have been promising: 1,045 arrests for document fraud and related offenses; 3,439 visa refusals and revocations; and 6,216 foreign law enforcement and security personnel trained.

In addition, DS has Special Agents assigned to Regional Security Offices (RSOs) at 165 U.S. diplomatic missions and consulates that have responsibility for an additional 104 constituent posts. Through the implementation of this Strategic Plan, DS will leverage this global network of international law enforcement partners to enhance its worldwide investigative capacity.

Domestically, DS Special Agents serve in field offices and resident offices in 25 cities across the country. DS Special Agents also participate in 26 Joint Terrorism Task Forces (JTTF) and 11 Document and Benefit Fraud Task Forces. DS's Global Pursuit Initiative assigns DS Special Agents to major international airports throughout the United States to assist the U.S. Department of Homeland Security (DHS) in investigating visa and passport irregularities. In conjunction with DHS's ongoing Secure Border Initiative, these DS Special Agents contribute valuable investigative assistance. Since 2004, these DS Special Agents have arrested 2,149 individuals on passport and visa fraud charges and related offenses in the United States.

## OBJECTIVE: EXPAND DS'S OVERSEAS CRIMINAL INVESTIGATOR PROGRAM

### DEPLOY DS SPECIAL AGENTS TO ADDITIONAL POSTS WITH IDENTIFIED HIGH LEVELS OF FRAUDULENT TRAVEL DOCUMENTS

In 2004, the Bureaus of Diplomatic Security and Consular Affairs signed a new Memorandum of Understanding for the assignment of DS Special Agents to conduct fraud investigations in consular sections abroad. This partnership has resulted in the deployment of 26 DS Special Agents (with an additional 7 in 2007) to consular posts that encounter high numbers of fraudulent travel documents. These Special Agents investigate travel document fraud and review irregular visa applications. They also develop partnerships with host countries' law enforcement officials to investigate, arrest, and prosecute those who produce and/or use fraudulent travel documents.

DS Special Agents augment visa security support by investigating suspect documents and visa/passport applications. DS Special Agents have access to law enforcement databases not generally available to consular personnel. They consult with their foreign law enforcement counterparts and question applicants based on broad knowledge of local and international law enforcement information. Integrating these capabilities will both improve and streamline the visa adjudication process.

DS's expertise in overseas operations and its impressive track record prove that the State Department's established infrastructure possesses the ability to deploy additional personnel quickly and efficiently. Using a comprehensive methodology, DS and CA have identified and prioritized additional posts with high volumes of fraudulent travel documents for future deployment of DS Special Agents. This expansion will increase the number of posts participating in the Visa and Passport Security Program and minimize their vulnerability to fraudulent travel documents.

### EXPAND PARTNERSHIPS WITH FOREIGN LAW ENFORCEMENT PERSONNEL

Expansion of the Program overseas will strengthen partnerships between DS Special Agents and host governments' law enforcement and border security personnel. Such enhanced partnerships will increase the numbers of investigations, arrests, and prosecutions of those who engage in travel document fraud. Continued success with Program partners will provide fertile ground for further training in the prevention and detection of travel document fraud, and enhance the coordination of regional strategies to combat terrorist travel. In addition, DS Special Agents will be uniquely positioned to identify foreign partners that require additional training, technical assistance, and legal and administrative reform in order to achieve long-term success.

## OBJECTIVE: ENHANCE DOMESTIC LAW ENFORCEMENT EFFORTS TO SUPPORT THE SECURE BORDER INITIATIVE

### APPOINT A VISA AND PASSPORT SECURITY PROGRAM COORDINATOR

As required by the IRTPA, the Assistant Secretary for the Bureau of Diplomatic Security has designated the Director of Investigations and Counterintelligence as the individual responsible for implementation of the Program. This position is staffed by a Special Agent in Charge who coordinates both domestic and international law enforcement operations and reports directly to the Assistant Director for Domestic Operations.

### ENHANCE DS DOMESTIC INVESTIGATIVE CAPABILITY

DS will continue to enhance its domestic criminal investigations program to fulfill the requirements of the Secure Border Initiative, especially in regions of the United States that historically have experienced high levels of travel document fraud. In the immediate post-9/11 era, DS initially expanded its liaison and task force efforts with several federal law enforcement agencies and intelligence organizations. Additional domestic personnel are required to support our local, state, and federal law enforcement colleagues and pursue leads generated by overseas investigations. This augmentation of DS resources reflects the Bureau's expanded mission in investigating and apprehending perpetrators of transnational travel document fraud.

### ASSIGN SPECIAL AGENTS TO KEY DOMESTIC PROCESSING SITES

The assignment of additional agents to CA's passport field offices, the National Passport Center, and the National Visa Center is critical to ensuring the timely investigation of travel documents thought to be fraudulent during the inspection and processing of visa and passport applications. Enhancing DS's presence at these centers will integrate thoroughly DS's law enforcement and CA's fraud-fighting efforts. This initiative also will augment and expand ongoing DS-CA efforts to investigate petition revocations and prosecute alien smugglers.

## EXPAND DS'S GLOBAL PURSUIT INITIATIVE

Through the Global Pursuit Initiative, DS Special Agents are assigned to major international airports in the United States to investigate irregularities in U.S. visas and passports. These DS Special Agents work in conjunction with Customs and Border Protection (CBP) inspectors and Immigration and Customs Enforcement (ICE) agents stationed at multiple ports of entry. Expansion of this program to 35 of the Federal Aviation Administration's (FAA) major international airports in the United States will enhance DS's ability to respond, investigate, and collect intelligence on trends in visa and passport violations. DS Special Agents will enhance CBP inspectors' and ICE agents' investigative capabilities through DS's worldwide law enforcement network.

## EXPAND THE CIVIL SERVICE CRIMINAL INVESTIGATOR PROGRAM

Criminal investigative programs require continuity to leverage the experience of an organization's special agents with their extensive network of local, state, and federal law enforcement colleagues. Although the Department's diplomatic mission requires DS to focus on international law enforcement and security programs, the success of the Visa and Passport Security Program can be achieved only through an effective domestic effort. Since 2004, DS has identified this need and committed itself to building a strong domestic foundation for its worldwide criminal program. In the past two years, more than 20 Civil Service criminal investigator positions have been created to provide continuity; an increased domestic criminal investigative capacity; and an augmented ability to respond to the needs of DS investigations and those of local, state, and federal law enforcement counterparts. In addition, DS will explore with the Department the possibility of establishing a pilot program for Foreign Service Special Agents to convert to the Civil Service and remain with DS. This initiative would allow DS to continue developing qualified law enforcement professionals and increase the ability of the organization to retain these valuable human assets.

## INCREASE DEDICATED LEGAL SUPPORT

DS's expanded global law enforcement program will require greater in-house legal assistance to address sufficiently the specific law enforcement needs of the Bureau. DS will seek to increase the number of Department attorneys dedicated to working on DS criminal law enforcement investigations and prosecutions and to enhance the attorneys' roles in providing legal counsel in applicable criminal law.

These attorneys will assist DS in coordinating DS criminal investigations with the U.S. Department of Justice (DOJ) and U.S. Attorney's offices across the country. DS also will seek funding for the support of designated prosecutors in selected U.S. Attorney offices throughout the United States to target and prosecute passport fraud crimes. This initiative reflects DS's management decision to [illegible] on these crimes with high [illegible] complexity, and resources to [illegible] dedicated attorneys to evaluate [illegible] travel documents and [illegible].

Additional legal staff will [illegible] in investigations [illegible] the ability of the Department to [illegible] documents and improve both DS [illegible] prosecutorial efforts. Congressional [illegible] been [illegible] [illegible] in the [illegible] [illegible] [illegible]

VISA AND PASSPORT SECURITY STRATEGIC PLAN
18
UNITED STATES DEPARTMENT OF STATE • BUREAU OF DIPLOMATIC SECURITY

## STRATEGIC GOAL 2

*Detect terrorist activity, methods, and trends that exploit international travel vulnerabilities.*

One of the fundamental findings of the 9/11 Commission's report was the failure of operational entities and intelligence agencies to coordinate their efforts and intelligence into a comprehensive assessment of national security threats. Effectively countering terrorist mobility requires an interagency apparatus that fosters the timely exchange of intelligence and information on travel document fraud and illicit travel. Tracking terrorist travel requires a unique blending of traditional resources of the law enforcement and intelligence communities. This synthesis can produce programs that use database and data-mining techniques and intelligence analysis that address threats from terrorist mobility and trends in fraudulent travel documents.

Since 9/11, the majority of the Department's efforts to counter terrorists' ability to travel have focused primarily on pretravel assessment and countermeasures. DS's monitoring of vulnerabilities identified during criminal investigations has resulted in the arrests of vendors and facilitators of fraudulent travel documents. CA, in turn, has transformed its application data procedures and interview standards; enhanced mandated advisories on aliens of special interest; and integrated watch list and biometric identifiers into the application process for visas and passports.

The Vulnerability Assessment Unit (VAU) in the Office of Fraud Prevention Programs is a joint DS-CA initiative. The VAU uses data-mining and risk-analysis techniques to detect anomalies and spot trends and patterns in visa and passport processing and potential breakdowns in internal controls; makes recommendations to address vulnerabilities; and provides investigative support to DS in visa and/or passport fraud and malfeasance investigations.

DS also has assigned DS Special Agents to liaison positions within multiple intelligence and law enforcement agencies—including the Federal Bureau of Investigation (FBI), the Central Intelligence Agency, NCTC, DHS, U.S. Marshals Service, and Interpol—to ensure the timely dissemination of DS intelligence and investigative information. The DS Visa and Passport Analysis Unit evaluates Department databases and reporting to identify potential criminal activity and provide actionable information to both criminal investigators and CA officials. Finally, DS has assigned staff to the Human Smuggling and Trafficking Center (HSTC) to support its role as a "clearinghouse" for intelligence on human smuggling and trafficking, as well as terrorist travel.

OBJECTIVE: OPTIMIZE THE HUMAN SMUGGLING AND TRAFFICKING CENTER'S ROLE IN OPERATIONS

REVIEW POLICY, FUNDING AND OPERATIONAL STAFF ASSIGNMENTS

CREATING A NEW LEADERSHIP ROLE FOR DS

## OBJECTIVE: ESTABLISH A CRIMINAL INTELLIGENCE CAPABILITY WITHIN DS

### EXPAND DS'S CRIMINAL INTELLIGENCE AND RESEARCH BRANCH

The DS Criminal Intelligence and Research Branch (CIR) was created in 2005 to collect, collate, and analyze criminal intelligence pertaining to terrorist travel and document fraud. The CIR disseminates information essential to the success of DS Special Agents' ability to conduct global criminal investigations involving document counterfeiting, imposters, processing irregularities, and related document fraud. CIR analysts review investigative information from a wide range of government and Department databases, such as the Consolidated Consular Database (CCD), to detect patterns of criminal activity related to U.S. travel documents.

The expansion of the CIR is essential to prevent, detect, and neutralize travel document fraud that enables individuals to enter the United States and/or other countries illegally. CIR operations have created an intelligence and research operations component within DS that can access sophisticated analytic tools, technical investigations equipment, and a network of legal and regulatory sources of information. CIR has become a focal point for DS's worldwide criminal program, serving as a clearinghouse for intelligence and information provided by DS's overseas and domestic criminal investigations.

### EXPAND THE INTELLIGENCE ANALYST PROGRAM

Over the past two decades, DS has used intelligence analysts to support its protective security responsibilities through its Intelligence and Threat Analysis Division and Overseas Security Advisory Council. Building upon these successful models, DS created the CIR intelligence analyst program to meet the needs of an expanding international criminal program. However, the current CIR headquarters intelligence staff is but one component of a comprehensive analysis program designed to process raw intelligence generated by overseas and domestic investigations.

Successful implementation of the CIR will require the deployment of intelligence analysts in response to the expansion of DS's worldwide enforcement initiatives. Assignment of analysts to overseas posts that encounter high levels of fraudulent travel documents, to CA fraud prevention programs, and to DS domestic field and resident offices will enhance substantially the Department's interbureau intelligence collection and dissemination efforts. Detailing analysts to the FBI, DHS, NCTC, and HSTC headquarters will ensure the timely exchange of intelligence on the vulnerabilities of U.S. travel documents and terrorist mobility. Finally, expanding the analyst program to the JTTFs and Fraud Benefit Task Forces will augment current DS participation and ensure that DS criminal intelligence is provided to domestic task forces targeting terrorist travel and travel document fraud.

## OBJECTIVE: ENHANCE INTERDEPARTMENT COOPERATION AND TRAVEL DOCUMENT VULNERABILITIES EFFORTS

### ENHANCE THE VULNERABILITY AND ASSESSMENTS UNIT

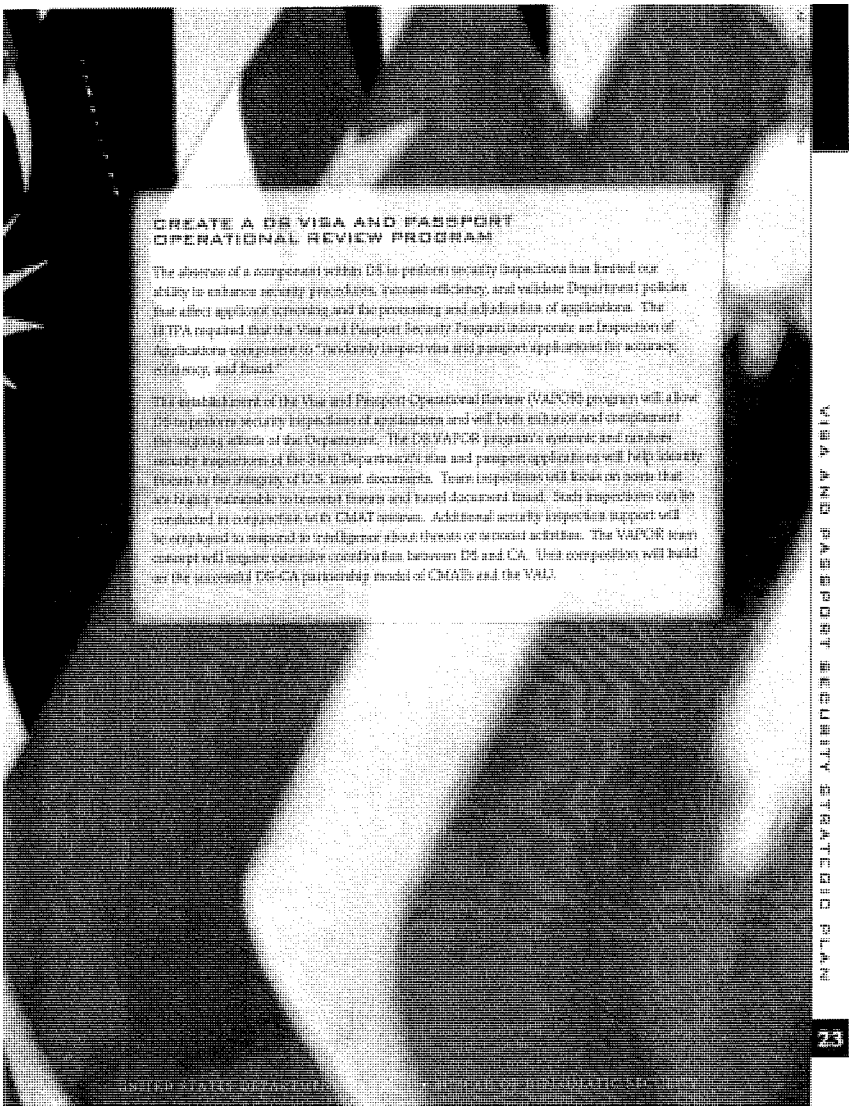
The joint DS-CA Vulnerability Assessment Unit analyzes consular data, systems, and processes to identify potential systemic vulnerabilities within issuance procedures and specific instances of processing irregularities. The CA-funded VAU currently is staffed by both CA officials and DS Special Agents and analysts, and is an excellent example of the DS-CA commitment to combating visa fraud.

The VAU continues to collaborate with technology developers to maximize data-mining efforts within the CCD. Application of database technology and techniques, such as statistical analysis and modeling, uncovers hidden patterns and subtle relationships within the CCD. VAU's risk analysis program can conduct system searches for specific, questionable real-time data as they are entered into the database and notifies VAU electronically of the exact circumstances of each visa issuance.

Automated reporting and other experience-based queries detect anomalies. Analysis of questionable patterns, which can detect anomalies and potential breakdowns in internal controls at posts, results in referrals to CA and DS for appropriate action. These initiatives have proven to be an effective and valuable tool for multiple DS investigations. Success for the VAU program will require a commitment to resources and technological innovation in order to keep pace with the growth of DS's international and domestic criminal programs.

### INCREASE DS PARTICIPATION IN THE CONSULAR MANAGEMENT ASSISTANCE TEAM REVIEWS

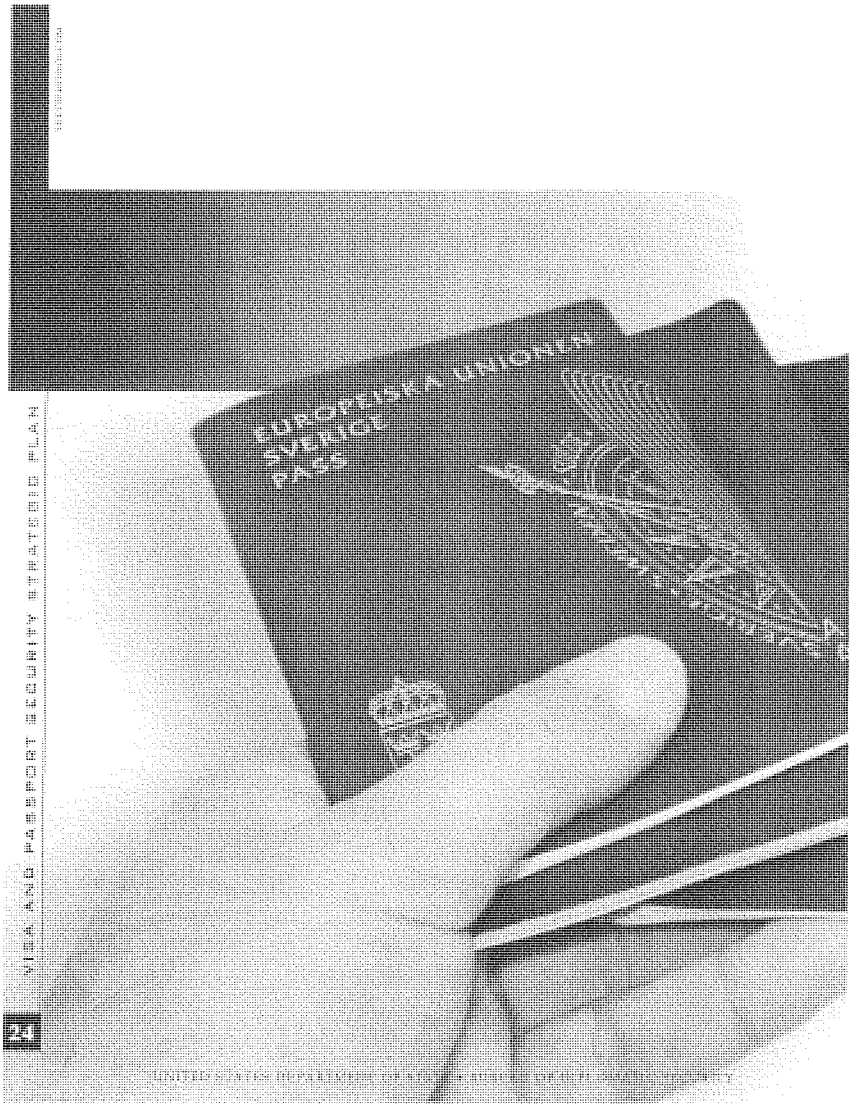
The Consular Management Assistance Team (CMAT) program was created by CA to assist consular sections in managing the myriad of changes, guidance, and operating procedures issued in the post-9/11 environment. CMATs conduct reviews of both consular operations and section management that significantly influence national security with increased resources. DS Special Agents will participate more frequently in these periodic reviews of visa and passport issuance operations and conduct follow-up investigations into related criminal violations. CMATs offer immediate guidance and solutions to difficulties that arise. Post-specific recommendations are shared throughout CA, maximizing the knowledge gleaned and lessons learned from the handling of challenging situations. The CMAT initiative is an innovative analysis-feedback program that has the potential to shape the Department's extensive quality-control and enhancement efforts.



## CREATE A DS VISA AND PASSPORT OPERATIONAL REVIEW PROGRAM

The absence of a component within DS to perform security inspections has limited our ability to enhance security procedures, increase efficiency, and validate Department policies that affect applicant screening and the processing and adjudication of applications. The IRTPA required that the Visa and Passport Security Program incorporate an inspection of Applications component to "randomly inspect visa and passport applications for accuracy, efficiency, and fraud."

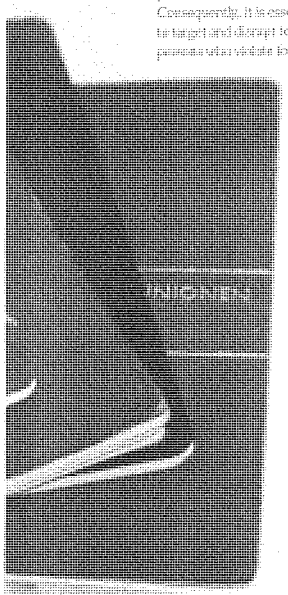
The establishment of the Visa and Passport Operational Review (VAPOR) program will allow DS to perform security inspections of applications and will both enhance and complement the ongoing efforts of the Department. The DS VAPOR program's systematic and random security inspections of the State Department's visa and passport applications will help identify threats to the integrity of U.S. travel documents. Team inspections will focus on posts that are highly vulnerable to terrorist threats and travel document fraud. Such inspections can be conducted in conjunction with CMAT teams. Additional security inspection support will be employed to respond to intelligence about threats or criminal activities. The VAPOR team concept will require extensive coordination between DS and CA. Unit composition will build on the successful DS-CA partnership model of CMATs and the VAU.


24
VISA AND PASSPORT SECURITY STRATEGY PLAN
EUROPEISKA UNIONEN
SVERIGE
PASS

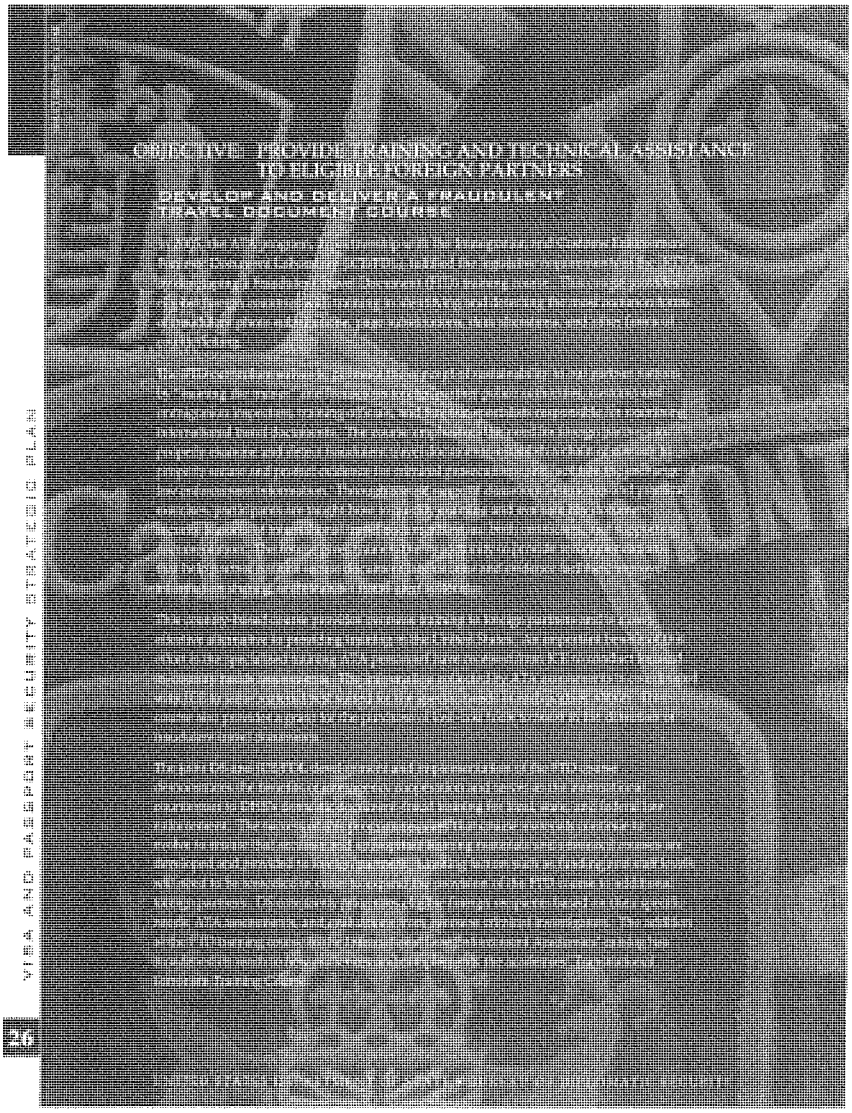
## Strategic Goal 3

*Disrupt terrorist efforts to use fraudulent travel documents through strengthening the capacities of foreign partners.*

Building foreign partner capability is vital to the security of the United States and our foreign partners. Successfully defending the homeland is best accomplished when terrorists are apprehended before they even reach the United States. This can only occur if our foreign partners have the training, technical assistance, and legal institutions needed to combat terrorism. Consequently, it is essential to identify countries that require assistance to enhance their ability to target and disrupt terrorist travel, detect fraudulent travel documents, and effectively prosecute [illegible] foreign anti-fraud laws, false document vendors, and terrorists.



DS has substantial experience in providing assistance to foreign partners engaged in the global war on terror. DS's Antiterrorism Assistance program (ATA) has generated notable success in training foreign law enforcement personnel. Training of foreign security personnel was conducted in Greece and Italy prior to the 2004 and 2006 Olympic Games. Extensive DS law enforcement and security training also has benefited such volatile countries as Afghanistan, Haiti, and Liberia. In 2006 alone, the ATA program sponsored 269 courses and technical consultations and trained approximately 4,600 students from 77 countries. Since its inception more than 20 years ago, ATA has trained some 55,000 students from 150 countries. Training curricula are tailored to the specific needs of the country and include courses such as Cyber-Terrorism, Airport Security, and Border Control. DS's ability to interact with police, immigration, and border authorities worldwide—coupled with extensive knowledge of foreign criminal justice systems and regional trends—places DS in a unique position to assess vulnerabilities in our foreign partners' efforts to combat terrorist travel.







**OBJECTIVE: PROVIDE TRAINING AND TECHNICAL ASSISTANCE TO ELIGIBLE FOREIGN PARTNERS**

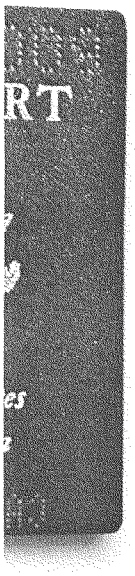
**DEVELOP AND DELIVER A FRAUDULENT TRAVEL DOCUMENT COURSE**

[illegible]

PROVIDE TECHNICAL ASSISTANCE
TO ELIGIBLE FOREIGN PARTNERS
FREE DESIGNATED CERTAIN ASSISTANCE
FUNDING FOR TRAINING AND TECHNICAL
ASSISTANCE PROGRAMS
STRENGTHEN FOREIGN PARTNERS
TERRORIST TRAVEL LEGISLATION EFFORTS
27
NATIONAL STRATEGY FOR MARITIME SECURITY
VISA AND PASSPORT SECURITY PLAN

PASSP
OFFIC
PASSP
DIPLOM
PASSP
PASSPO
United Stat
of America

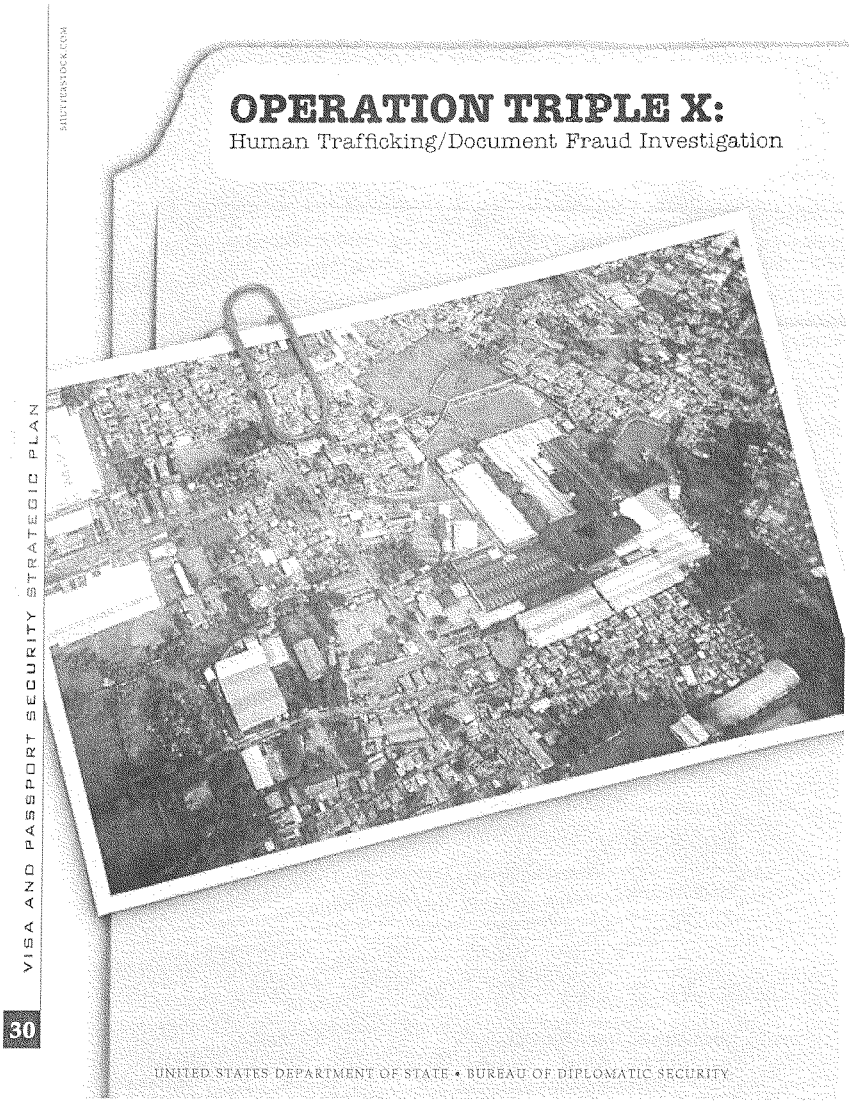
## CONCLUSION



The Visa and Passport Security Strategic Plan does more than respond to the requirements of Section 7218 of the Intelligence Reform and Terrorism Prevention Act. It does more than address vulnerabilities brought to light by the 9/11 hijackers' use of U.S. travel documents. This Plan provides a comprehensive blueprint for three proactive and integrated strategies to prevent the fraudulent production, manipulation, and acquisition of U.S. visas and passports. Wherever the U.S. Department of State issues travel documents, DS has the authority to investigate travel document fraud. Additions to DS's analytic, investigative, and training resources—as well as a vigorous process review—are essential to create and maintain a viable Visa and Passport Security Program.

The U.S. Department of State constantly is evolving and transforming. DS has always been a part of this and past transformations, but there is an additional dimension today. The entire U.S. Government has been grappling with a means to prevent terrorist travel. DS has moved forward and created 26 overseas criminal investigator positions; established and staffed a new Criminal Intelligence and Research Branch; and expanded its Civil Service Special Agent cadre. CA established Consular Management Assistance Teams and a number of other security countermeasures to protect the integrity of U.S. visas and passports and the processes through which they are issued. DS's ATA program established a document fraud course designed to help our allies detect and deter terrorists before they reach the United States.

Over the next three years, successful implementation of the Program will be dependent upon the provision of significant new resources, to include additional DS Special Agents, intelligence analysts, Foreign Service national investigators, and support staff to build upon this strong foundation. With Special Agents assigned to 200 overseas posts, DS and our foreign partners will be able to combat terrorist travel, document fraud, and human smuggling and trafficking directly at the source of these illicit activities. The Visa and Passport Security Program outlined in this Strategic Plan will position the Department of State as the most capable, best prepared, and flexible organization to anticipate and respond to the challenges of combating terrorist travel and ensuring the integrity of U.S. travel documents.


SHUTTERSTOCK.COM
OPERATION TRIPLE X:
Human Trafficking/Document Fraud Investigation
VISA AND PASSPORT SECURITY STRATEGIC PLAN
30
UNITED STATES DEPARTMENT OF STATE • BUREAU OF DIPLOMATIC SECURITY

# APPENDIX

Operation Triple X is a joint undercover operation by the U.S. Department of State's Bureau of Diplomatic Security and the Indonesian National Police (INP) to target Indonesian criminal syndicates involved in counterfeiting travel documents. These criminal syndicates were involved in extensive U.S. visa fraud activities, sophisticated document fraud, illegal immigration, production of counterfeit Indonesian passports, alien smuggling (throughout Indonesia, Malaysia, the Philippines, Thailand, Singapore, and Brunei), pedophile operations, trafficking in persons (women and children), drug trafficking, gun trafficking, and money laundering. The undercover investigation, which began in February 2005, also revealed that a few of these criminal Indonesian syndicates had a nexus to the terrorist network known as Jamal Islamyia and other Muslim extremist groups operating in Southeast Asia.

## WHY SURABAYA?

Surabaya is the main shipping port on the eastern end of the Indonesian archipelago and home to Indonesia's eastern navy fleet. Surabaya has a large concentration of brothels located in the heart of the city, with an estimated 14,000 women and children working in them. Surabaya is a central hub for human trafficking; illegal immigration; and timber, shrimp, and textile smuggling. Criminal syndicates are well established and operate openly in the city, bribing corrupt immigration and police officials. Jamal Islamyia and other Muslim extremist groups have taken advantage of the widespread corruption and criminal syndicates to further their causes.

The success of Operation Triple X is all the more remarkable considering that the investigation took place in an environment of direct and continuous terrorist threat to U.S. diplomatic facilities and personnel operating in Indonesia. Both the U.S. Embassy in Jakarta and the U.S. Consulate General in Surabaya were closed temporarily several times in 2005 and 2006 because of terrorist threats.

In February 2005, DS Special Agents from the Regional Security Office (RSO) at the U.S. Embassy in Jakarta and Consulate General in Surabaya began to coordinate an international criminal task force at both the national and local levels to shut down 12 major criminal syndicates that had been identified as operating across the archipelago. The initiation of the investigation began with the State Department's Consular Services' fraud coordinators identifying suspected counterfeit documents and alerting the RSOs. The RSO in Surabaya researched visa applications from three previous years, including files, notes, correspondence, and fraud coordinators' files. They also interviewed consular officers. Patterns and trends began to emerge.

The RSO began to interview all applicants for U.S. visas who had submitted documents suspected to be fraudulent. Many of these interviews provided valuable information confirming the rampant nature of criminal syndicates involved in counterfeiting travel documents and details of their operations. The RSO coordinated closely with Indonesian law enforcement and legal authorities. The first series of raids and arrests began in May 2005.

Twenty-one subsequent raids by the INP resulted in 84 arrests, including an Indonesian immigration official. The Indonesian prosecutor's office has charged and convicted all 84 arrested individuals under Indonesian fraud statutes. Evidence collected consisted of more than 4,800 fraudulent documents, including Indonesian passports; U.S. visas and passports; Indonesian national identification cards; marriage, birth, and family records; and vehicle registrations and driver's licenses. The Indonesian National Police also seized numerous computers, names of U.S. businesses hiring illegal immigrants, Indonesian and third-country official stamps, original and

unused blank Indonesian passport booklet covers with biographical data pages, reflective security laminates, and passport pages. More than 8,000 individuals were identified as using the services of these criminal syndicates.

These raids and arrests also uncovered the names of 100 individuals who successfully entered the United States through fraudulent means. Law enforcement officials in the United States subsequently have arrested several of these illegal aliens. One individual attempted to smuggle automatic weapons from Surabaya to Los Angeles, California. Two additional subjects were apprehended in New Mexico with 15 counterfeit Indonesian passports, Social Security cards, and New Mexico driver's licenses. These two individuals were attempting to open 30 separate checking accounts at banks in the state.

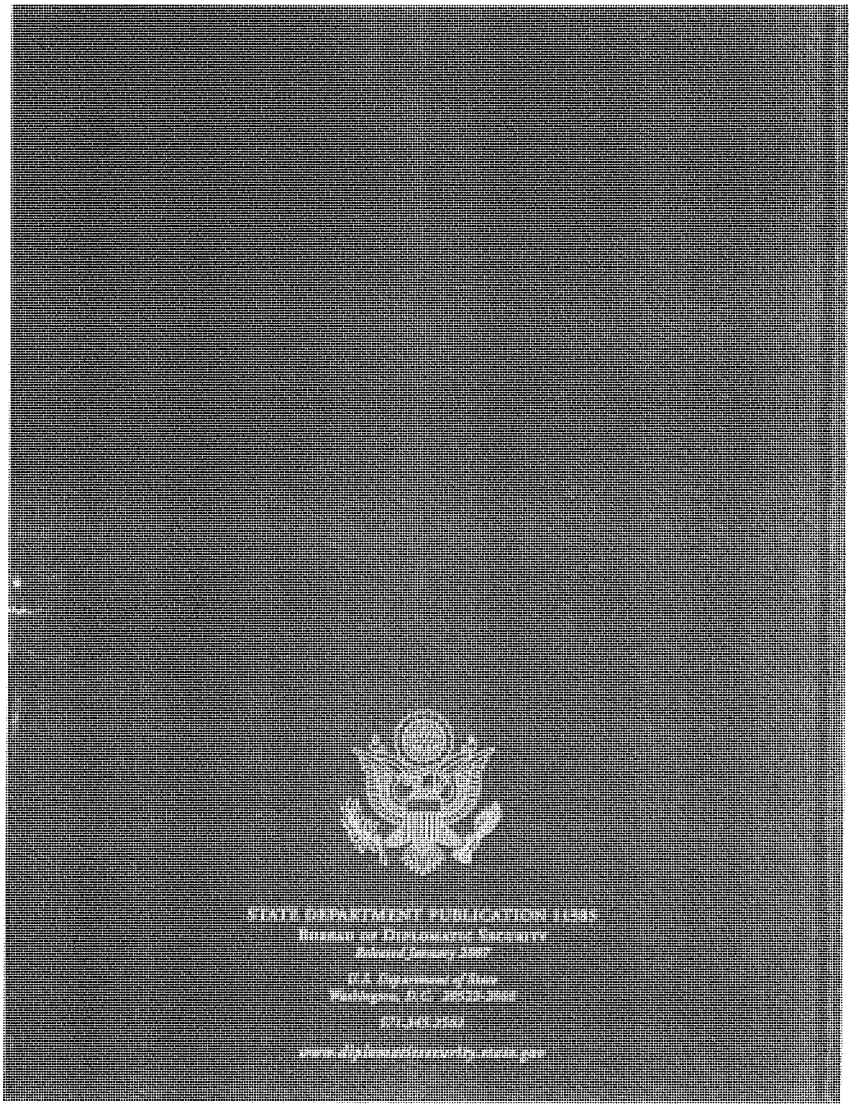
Operation Triple X revealed that criminal syndicates in Indonesia were selling counterfeit U.S. visas and other fraudulent documents to citizens of Indonesia, Thailand, Malaysia, the Philippines, China, and Vietnam for illegal entry into the United States. The fraudulent documents were used to obtain U.S. visas, immigration green cards, and U.S. Social Security cards. Fiscal accounting records obtained in one police raid show that one of these criminal syndicates made $3 million during a three-month period.

DS Special Agents in Indonesia identified many of the techniques used by the syndicates. Most striking was the fact that many of these groups were openly advertising their counterfeiting services in the local newspapers under advertisements for travel agents. Most of these purported travel agents operated as legitimate fronts for various criminal activities.

Some of the high-quality counterfeit replicas of Indonesian passports, national identity cards, birth and marriage certificates, bank booklets, and bank statements were provided with the help, knowledge, and assistance of corrupt immigration officials and police. Criminal enterprises charge $3,000 to $10,000 for their counterfeiting services. Price ranges depend on the quality of the fraudulent documents and the services purchased. Documents to create a completely new identity could cost $10,000. Most of the U.S. visa applicants were "coached" on how to prepare for their interviews. When an applicant arrived for the interview, he or she would provide all the fraudulent documentation (i.e., employment letter, symposium letter, business license, business tax form, valid Indonesian passport with overseas visas to other Southeast Asian countries, birth certificate, bank booklet or statement) to the consular officer.

The DS-INP team shut down these international criminal syndicates through intensive and meticulous investigations, close liaison with Indonesian officials, and prosecution of the cases. It took extraordinary planning and dedication by all of the DS Special Agents involved. The DS Special Agents conducted this operation with diligence and tenacity, while protecting U.S. diplomatic staff and facilities throughout the Indonesian archipelago.

KARTU TANDA PENDUDUK
REPUBLIK INDONESIA
PENCATATA
KUTIPAN
AKTA KELAHI
PASPOR
REPUBLIK
INDONESIA


STATE DEPARTMENT PUBLICATION 11068
Bureau of Diplomatic Security
Revised January 2007
U.S. Department of State
Washington, D.C. 20520-6808
(703) 875-7690
www.diplomaticsecurity.state.gov

**Prepared Testimony of Brian Zimmer**
**Senior Associate, Kelly, Anderson & Associates**
**Former Senior Investigator,**
**U.S. House of Representatives, Committee on the Judiciary**

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

**On**

# "Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents"

**Washington, DC**
**May 2, 2007**

## Introduction

Chairman Feinstein and Ranking Member Kyl, thank you for the opportunity to appear before the Subcommittee today and to share with you my thoughts on strengthening the security of international travel documents.

I am a Senior Associate at the consulting firm of Kelly, Anderson and Associates.[1] In the recent past, I worked directly with Members of Congress and Congressional staff on a number of important bills that strengthened travel document security. These included: the Enhanced Border Security and Visa Entry Reform Act of 2002, Identity Theft Penalty Enhancement Act of 2004, the Intelligence Reform Act of 2004, and the REAL ID Act of 2005.

As the senior investigator for the House of Representative's Committee on the Judiciary from 2001 through 2006, I conducted field oversight on the actual inspections of travel documents at our ports of entry to better understand the operational challenges faced by front-line personnel, and to understand weaknesses in our system that could be exploited by terrorists, criminals, and individuals engaged in fraud.

The Subcommittee's discussion on strengthening the security of international travel documents is timely: from this vantage point, we can evaluate the effectiveness of some of the reforms proposed by Congress and the efforts of the Administration and the Department of Homeland Security (DHS) to implement those reforms. For example,

[1] Among the clients of Kelly, Anderson and Associates are both government agencies and companies who have interests in secure document technology and identity document inspection. This testimony is submitted in my personal capacity.

individual travelers from Visa Waiver Program countries who fail to meet the biometric passport requirements are, in fact, being denied entry to the U.S., when traveling without a visa; and U.S. citizens are being issued the new highly secure passport with a stored digital image.

If one could envision homeland security measures to prevent attacks and subversion by foreign terrorists as a patchwork quilt, it could be seen that many of the patches which were absent before 9/11 have been put in place. The premise that identity documents need to be physically very secure, very counter resistant, and issued to people only after a thorough adjudication and authentication of source identity documents, is now generally accepted. At the same time, some important security patches are still missing, and others in place are only stop-gap measures and requiring more work. The missing "security patch" of greatest concern to me is the lack of substantial use of identity card reading technology to authenticate documents and confirm their relationship to the bearers at ports of entry and transportation terminals. Another "security patch" that continues to be put on the back burner is the application of exit controls at every port of entry.

However, I offer these concerns while recognizing that the Administration is faced with funding shortfalls and the need to balance priorities, and is often stymied in identifying practical solutions at reasonable cost. It is inherent in the changing nature of our terrorist opponents and their increasing sophistication that we will need to continue to work on closing holes in the blanket of homeland security.

**Accomplishments**

In my view, much has been accomplished to interrupt terrorist travel, and worthwhile initiatives have been undertaken by the Administration to improve the security of travel documents, some of which are the result of Congressional mandates contained in the aforementioned bills.

In an appendix to my testimony, I have listed the most important pieces of federal legislation since 2001 requiring security improvements applicable to identity documents issued by federal and state agencies. Because the foundation for international travel documents issued by the United States government is highly dependent on the identity authentication adjudication by the states in the course of driver's license issuance and birth certificate issuance, the REAL ID Act is included.

Here are some of the laudable accomplishments by the Administration and DHS:

- US Visit – where passports are compared to the biometrics of the passport bearer, frauds are immediately identified and a reliable record is stored.
- Significant improvements in the compilation of terrorist watch lists, and of the application of these watch lists to passenger lists as filters to international air travelers' identification through passports and passenger manifests.

- Enforcement of biometric passport requirements on countries participating in the Visa Waiver Program, along with on-site inspection of issuance processes of these same countries.
- Issuance of a new, more secure passport, with many features that make it highly counterfeit resistant. The addition of a chip, which stores the same data displayed on the photo page along with a digital photograph, enables inspectors to confirm that the passport bearer is the same person to whom it was issued. The read range of several centimeters, along with shielding material and the basic access control (BAC), will help to safe guard the stored data on the chip from would be data skimmers.
- Initiation of a world wide program, working together with INTERPOL and with the European Union and Visa Waiver Program countries, to collect data about lost and stolen passports that can be employed to identity imposters and to recover passports from thieves and document brokers.
- The pending introduction of a wallet sized "PASS Card" for border crossings to Canada, Mexico, the Caribbean, and Bermuda, hopefully also with a high level of physical security built into the card.
- Establishment of federal anti-counterfeiting task forces across the country. Results of their investigations are now evident with prosecutions of counterfeiting rings. These enforcement actions are equally important to security improvements in travel documents.
- A growing level of investigations and arrests by federal agents targeting those who sell counterfeit identity documents through the internet.
- Increased prosecutions by the Department of Justice and the U.S. Attorney's offices under both the Identity Theft Penalty Enhancement Act and the anti-fraud provisions of the REAL ID Act.

There has been important guidance by the Congress to the Administration through enabling legislation, and there remains the need for continued oversight of the Administration's efforts to complete the task list set by Congress.

It is my assessment that the Administration is working hard but finding it difficult to manage so many complex tasks. Homeland Security was not a priority before 9/11 and many important security improvements remain incomplete.

## Cautionary Observations

U.S. Passports issued prior to the latest passport will remain in circulation and active use for border entry until 2016. There is a very strong international demand for stolen and lost U.S. passports, and it is likely the demand will become greater and the black market value higher for the "older" passports which can be more easily altered.

This means that safeguards against people using validly issued passports purchased on the fraudulent document markets needs to increase. Customs and Border Protection will need to be much more proactive in identifying when an imposter is carrying a passport

with a "look alike" photo that closely resembles the bearer. Machine readers are available to government purchasers that can greatly assist in such a determination.

Any major Mexican city close to the border hosts a fraudulent document market where people wishing to cross the U.S. port of entry as imposters can purchase or sometimes "rent" U.S. passports, B1/ B2 biometric border crossing cards, and the passports of visa wavier countries. The price ranges from a few hundred dollars for a California driver's license to tens of thousands of dollars for a valid U.S. passport with an expiration date five years or more in the future and with a photo closely comporting to the imposter. It's a rational market, following the best economic principles of supply and demand, with values based on reliability and duration of use. The black market depends on the continued reliance by U.S. border inspectors on spot checks and expedited inspections.

There was a time that access to these markets was restricted to those who appeared to be natives of Mexico and Central America, but with the growth in other foreign visitors to Mexico on the many charter flights from around the world, anyone who has the money can make the necessary arrangements. It would be imprudent for Congress to believe that the major terrorist organizations lack the money, sophistication or motivation to avail themselves of these document markets.

Beginning in 2006, there was an initiation of "100%" document inspection at nearly all of the ports of entry on the U.S. border with Canada. While the less frequented ports of entry experienced little back up, the busiest ports were highly impacted and the requirement was soon relaxed.

At the majority of the ports of entry on the border with Mexico, only a small percentage of those crossing the border are subject to a "real" documents check.

This lack of document inspection is risky business. To compound the risk, no one who visits the United States and then leaves through a port of entry is subject to an exit control inspection, with or without a document check. That this situation continues nearly six years after the 9/11 attacks, and four years after our country became deeply involved with wars in Afghanistan and in Iraq, should be a major concern for the Senate. In these foreign wars, our military opponents actively practice terrorism and promote anti-American terrorism on a world scale, yet we have no exit control system in place to allow us to determine whether foreign visitors are actually leaving the country.

Until our ports of entry on the border are reconfigured to allow universal document checks (at least during periods of high security concern) and all documents are systematically confirmed, imposters entering with fraudulent, altered and stolen travel documents, such as lost and stolen U.S. passports, will pass with impunity.

Primary reliance on remote databases is not a good idea, in the absence of document inspection, whether those databases are accessed as the result of an IC chip in a card with a secure reference number being read by an RFID scanning device, or as the result of a human inspector punching a number into a computer terminal. Accessing a remote

database to confirm that an identity document presented to an inspector is a valid and authentic document and it belongs to the person presenting it, is a demonstrably valid idea. That is, remote databases operating under a high level of system security, together with other anti fraud measures, are an excellent means of providing an additional level of safety, but it should not displace the personal confirmation of trained and experienced inspectors. The greatest risk with a central database accessible by a reference number is this: if the security of the database is significantly compromised, the individual access numbers contained on the RFID chips will likewise be compromised, opening the door to large scale counterfeiting of the cards unless the cards contain significant countermeasures to defeat counterfeiting.

There are reliable and secure documents used for international travel. One of the most reliable security features is the optical memory strip contained on the B1/B2 biometric border crossing cards and on Permanent Legal Resident cards. It is critical that the Department of Homeland Security continue to make border crossing cards highly physically secure to prevent counterfeiting. Successful security features demonstrated to be counterfeit resistant should not be lightly thrown away.

An example of how easily this can happen is offered by the Employment Authorization (EAC) Card provided by DHS' U.S. Citizenship and Immigration Services (USCIS). Unlike the "Green Card" or Permanent Legal Resident Card, the EAC is widely counterfeited. Primary customers include scofflaw employers wishing to conceal illegal immigrant employees working for them, as evidence that the employers were "duped" by the cards. Such cards are now available to English speaking customers through the internet. USCIS could have elected to employ counterfeit-resistant technology in the EAC to limit or potentially prevent this counterfeiting, but whether through a misguided effort to cut costs or limited vision by the program leads, USCIS elected to take the "cheap" route, leading to an insecure document. While this is not a travel document, a counterfeit EAC allows a person not lawfully present to remain undetected in the U.S., and facilitates illegal employment.

This country is at serious risk from foreign terrorists. Key priorities should be: Travel documents presented at land ports of entry need to be inspected by human eyes or a highly effective automated means of inspection; all federal customs and immigration inspectors at all our ports of entry must be trained to recognize counterfeit documents; state of the art document authentication readers must be placed at primary port of entry stations to authenticate frayed or potentially alter documents; and Transportation Security Administration inspectors at our airports must be trained to identify fraudulent documents and to recognize and refuse to accept ID cards that do not meet reasonable physical security and identity adjudication standards.

## Conclusion

The Administration has made important strides over the past five years toward meeting Congressional mandates addressing secure travel and identity documents. There remains a high risk that foreign terrorists will visit harm on the United States. The greatest

vulnerability is in the lack of standards for both foreign travel documents and U.S. identity documents with regard to traveler inspection at airports and land borders. This risk is compounded by the absence of quality control and inspection integrity systems. The identity authentication that precedes issuance of passports by the United States is largely dependent upon source identity documents issued by the states, and that remains a serious vulnerability. Congress should support travel and identity document improvements with federal funding, including providing grants to states seeking to become compliant with the REAL ID Act.

**Appendix to Testimony of Brian Zimmer, May 2, 2007**

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

## U.S. Federal Laws since 2001 which impact travel identity document Security and the need to authenticate those documents as belong to the bearers.

The following is an unofficial, informal, and probably incomplete compilation of key features and provisions of laws passed by Congress since 2001 that address identity and travel documents (both international and domestic).

It includes the USA PATRIOT Act (2001), the Enhanced Border Security and Visa Entry Reform Act of 2002 (Also Known As the Border Security Act), the Identity Theft Penalty Enhancement Act (2004), the Intelligence Reform Act (2005), and the REAL ID Act (2005).

### USA PATRIOT Act

Title Three of the USA PATRIOT Act was the first step in establishing the principle that both businesses and government inspectors should be able to authenticate the identities of U.S. nationals and of foreign visitors. It focused on better identification security as a key element in combating foreign terrorists entering and remaining in the U.S. It also required federal authorities to use biometrics for HAZMAT commercial drivers, which strengthened the principle of employing objective data beyond source identity documents to authenticate the holder of an identity document. It extended the principle of identity authentication for federally regulated financial enterprises as a means of identifying potential terrorists and the supporters of terrorism.

**The PATRIOT Act Required a Technology Standard to Confirm Identity**

Section 403(c) required federal agencies to work through the National Institute of Standards and Technology (NIST) to develop and certify a technology standard, although the term biometric was not included, to verify the identity of foreign visitors to the U.S.

The same section also required the creation of a cross agency computer system that would have a common (biometric) set of visa holder identifiers so that federal law enforcement officers could share law enforcement and intelligence information necessary to confirm the identity of visa applicants and issued visas. In short, it set the basis for federal law enforcement to be able to physically identity people who had legally entered the country. It also required that the new system would be accessible to the entire range of federal officials who actually interact directly with foreign visitors -- consular officers

issuing visas, border inspectors, and federal law enforcement officers such as the FBI who would investigate or otherwise need to identify aliens lawfully admitted to the United States.

Comment: This provision set the basis for common technology elements in identity management systems across federal law enforcement, which in turn affects the data available to generate identity and travel documents and the information available to authenticate the document holders with the documents.

**Checking Visa Applicants' Fingerprints Against FBI Systems**

Section 405 required a feasibility report on what level of enhancement of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) or other identification systems would be required to better identify a visa applicant, and to determine whether he/she might be wanted in connection with a criminal investigation in the United States or abroad, prior to issuing of a visa and check fingerprints at the entry or exit from the United States by that person.

Comment: This provision established the premise of U.S-VISIT, which now captures, upon entry, the fingerprints of foreign visitors save those from Mexico and Canada. Regrettably, there is still no such application upon exit, and therefore no reconciliation of records to identify visa overstays who might easily be foreign terrorists.

**Enhanced Border Security Act and Visa Entry Reform Act**

The Border Security Act was directed to impose requirements to find solutions to a lengthy list of homeland security problems, including especially insecure documents and inspection processes. It also set the stage for the DHS Bill and Intelligence Reform.

**Expanded Pre-inspection of Travelers and Anti-Fraud Measures at Foreign Airports**

Section 101(c) authorized funding to train immigration officers to use the appropriate lookout databases, to monitor passenger traffic patterns, and to expand the Carrier Consultant Program. This program assigns immigration officers to assist air carriers in the detection of imposters and document fraud at those foreign airports from which a significant number of aliens arriving at U.S. ports of entry without valid documentation departed, but where no pre-inspection station currently exists.

**Adjudication and Authentication of Foreign Documents Presented by Visa Applicants**

Section 101(d) directed the Secretary of State to implement enhanced security measures for the review of visa applicants which inevitably, but not specifically, includes the identity documents presented by them.

**Imposing a Penalty on Bearers of Non Machine Readable Passports**

Section 103 sets the machine-readable visa (MRV) fee charged by the State Department at the higher of $65 or the cost of the MRV service, to be determined by the Secretary of State after conducting a study on such costs. This section also permits the Department to levy a $10 surcharge when an MRV is placed in a non-machine-readable passport.

**Technology Standard Deadline for Visa Applicant Identity Authentication**

Section 201 accelerates the deadlines contained in Section 403(c) of the USA PATRIOT Act for the development of a technology standard to confirm the identity of visa applicants and for the delivery to Congress of a corresponding report on this technology standard.

**Visa Biographical Information at the Border**

Section 301 requires making available to border immigration inspectors at ports of entry an electronic version of the alien S visa file, which allows visual comparison of the visa file to the bearer of the passport within which the visa is contained.

**One System for Visitor Inspection and Data Records**

Section 302 essentially set the parameters of today's US-VISIT program, requiring the establishment of an entry/exit data system at all U.S. ports of entry and consular posts; establishing a database that compiles the arrival/departure data from all travel, entry and identity documents possessed by aliens; and making interoperable all of the security databases involved in determining the admissibility of aliens.

**Machine Readable, Tamper Resistant International Travel Documents**

Section 303 required the U.S. government and the participating countries of the Visa Waiver Program (VWP) to begin issuing machine-readable, tamper-resistant, travel documents with biometric identifiers no later than October 26, 2004. In addition, also by October 26, 2004, the government of each country participating in the VWP was required to certify that it has a program to issue its nationals the same type of documents, and all individuals entering the U.S. under the VWP beginning on that date must present a passport meeting the above-described requirements unless the document was issued prior to that date. This section also requires the installation of biometric readers and scanners at all ports of entry by October 26, 2004 (the dates for compliance were extended by subsequent provisions, but all requirements have now been substantially met).

**Establishment of National Standards for Biometric Identifiers**

Section 303 also required that, within 180 days of enactment, the Attorney General, the Secretary of State, and the National Institute of Standards and Technology (NIST) submit to Congress a comprehensive report assessing the actions that will be necessary to

achieve the above technology requirements. This section also authorized funding to carry out its requirements. The result was the establishment of technology standards for fingerprints and digital facial images by NIST, which worked together with federal agencies to complete them. This was a very important first step in building the foundation for exchanging data among federal traveler and foreign visitor inspection systems, as well as with information stored in watch list repositories.

**Reporting the Theft of Blank Passports**

Section 307 stipulated that before a country may participate or continue to participate in the VWP, it must certify that it reports on a timely basis to the U.S. government any theft of blank passports. If the Department of Homeland Security and the Secretary of State jointly determine that a VWP country is not reporting the theft of blank passports, the country will lose its ability to participate in the VWP.

Comment: The Administration needs to work hard to develop an information system that delivers information about all U.S. and foreign stolen passports to border inspectors at primary inspection stations.

**Tracking System for Lost and Stolen Passports**

Section 308 requires the Attorney General, in consultation with the Secretary of State, to enter stolen passport numbers into the interoperable electronic data system within 72 hours of notification of loss or theft.

Comment: The lack of progress on this requirement has to be considered a significant missed opportunity to improve homeland security.

**Employment Authorization Documents (Secure IDs) for Refugees and Asylees**

Section 309 provides that refugees, upon admission to the U.S., and asylees, upon a grant of asylum, must be provided an employment authorization document (EAD) that bears their fingerprint and photograph.

Comment: This remains a work in progress. More needs to be done to raise the quality of EADs to the equivalent security of that of Permanent Legal Resident cards, and to require all foreign guest workers to hold the secure cards. Currently, there is a proposed option to charge each immigrant $109 in order to receive their EAD. The fee should be mandatory, and the fees collected should be utilized to provide a highly counterfeit-resistant document.

## Identity Theft Penalty Enhancement Act

This Act mandates sentences of two years imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during, and in relation to, specified felony violations (including felonies relating to theft

from employee benefit plans and various fraud and immigration offenses), and five years imprisonment for knowingly taking such action during and in relation to specified felony violations pertaining to terrorist acts, in addition to the punishments provided for such felonies.

The Act prohibits a court from: (1) placing any person convicted of such a violation on probation; (2) reducing any sentence for the related felony to take into account the sentence imposed for such a violation; or (3) providing for concurrent terms of imprisonment for a violation of the Act and any other violation, except, in the court's discretion, an additional violation of the section.

It expands the prior identify theft prohibition to: (1) cover possession of a means of identification of another with intent to commit specified unlawful activity; (2) increase penalties for violations; and (3) include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism.

Rigorous enforcement of identity theft crimes at every level of law enforcement is extraordinarily important. As international cooperation increases to combat terrorism, al-Qaeda and other terrorist organizations will increasingly turn to stolen identities to hide themselves from law enforcement.

Foreign terrorists are well aware of how to falsify identities in the United States. Five Social Security numbers associated with some of the 9/11 terrorists were frauds never issued by the Social Security Administration, yet were sufficient to obtain driver's licenses and state issued identity documents from the states.

According to the official House Report on HR 1731, one terrorist used a Social Security Number assigned to a child, and four of the terrorists were associated with multiple Social Security numbers. The same report quotes an FBI agent "terrorists have long utilized identity theft as well as Social Security number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain driver's licenses, and bank and credit card accounts, through which terrorism is facilitated."[2]

## Intelligence Reform Act

**Fraudulent Document Recognition**

Section 7203 amends the Enhanced Border Security and Visa Entry Reform Act of 2002 to require consular officer training in document fraud detection.

The Act directs the Secretary of State, in coordination with the Secretary, to: (1) conduct a survey of each diplomatic and consular post at which visas are issued to assess the extent to which fraudulent documents are presented by visa applicants; and (2) not later

[2] H.R. Rep. No. 108-528 (2004)(Conf. Rep.).

than July 31, 2005, identify the posts experiencing the highest levels of fraud and place in each such post at least one full-time anti-fraud specialist unless a DHS employee with sufficient training and experience is already stationed there.

**Lost, Stolen & Fraudulent Passports**

Section 7204 directs the President to seek international cooperation to: (1) share information on lost, stolen, and fraudulent passports and other travel documents; (2) establish and implement a real-time verification system for such documents; and (3) encourage criminalization of certain conduct that could aid terrorist travel. It also requires the President to submit annual progress reports on such efforts.

Comment: Great progress has been made through the offices of Interpol to collect the data, with over 120 countries now participating in providing data on lost and stolen passports. Interpol continues to advocate use of its database for detecting imposters and recovering passports. The U.S. still has not met the requirements of this section, despite the success of countries like Switzerland, which now effectively uses the system's data to identity and arrest imposters. What is particularly concerning about this lapse is that the inspection of persons entering with U.S. passports is not subject to any equivalent to the U.S-VISIT system, which makes it relatively easy for imposters to pass through our ports of entry undetected.

**Lost in Translation: Arabic & Chinese Names**

Section 7205 expresses the Congressional intent that the President seek to enter into an international agreement to modernize and improve standards for the translation of names into the Roman alphabet in order to ensure common spellings for international travel documents and name-based watch list systems.

Comment: This is a subtle but very important requirement for the federal agencies which rely on passports and visa information. The international community has standards for translations of names from native alphabets into the Roman alphabet, which the English, Spanish, French, and all other major European languages use. However, these rules-based standards have proven to allow, and sometimes create, errors in translation. It is critical that these standards improve to facilitate correct identification of suspected terrorists whose native language requires alphabetic translation and to avoid misidentification of people with similar names.

**Visa Waiver Program Country Accountability for Secure Documents**

Section 7207 required the Secretary of State, no later than October 26, 2006, certify which of the countries designated to participate in the Visa Waiver Program are developing a program to issue machine readable, tamper-resistant visa documents that incorporate biometric identifiers.

Comment: Implementation and enforcement of this provision by the Department of Homeland Security has been put in place and is a significant success for the Administration.

**Biometric Passports for U.S. Citizens by 2008**

Section 7209 directs DHS, consulting with the State Department, to implement by January 1, 2008, a plan to require biometric passports or other secure passports for all travel into the United States by U.S. citizens and by categories of individuals for whom documentation requirements were previously waived.

Comment: This requirement looks as though it will be met on time. It is important that technology supported by facial recognition software be employed at all U.S. ports of entry, especially on the land borders, as soon possible to support authentication of digital images with the face of the person presenting the passport.

**Verification of Passports & Higher Standards**

Section 7210 Expresses the Congressional intent that the U.S. Government should: (1) exchange terrorist information with trusted allies; (2) move toward real-time verification of passports with issuing authorities; (3) where practicable, conduct passenger prescreening for flights destined for the United States; (4) work with other countries to ensure effective airport inspection regimes; and (5) work with other countries to improve passport standards.

Comment: The Department of Homeland Security, together with the Department of State, is proceeding with initiatives that incorporate these objectives. Congress should continue to exercise oversight to evaluate the results of these initiatives and the current level of risk from weak passport regimes among foreign countries.

**Secure Birth Certificates**

Section 7211 requires the Secretary of Health and Human Services (HHS) to establish minimum standards for birth certificates for use by Federal agencies for official purposes. It also prohibits Federal agencies from accepting nonconforming birth certificates beginning two years after promulgation of such standards, and it requires States to certify compliance with such standards.

Comment: This requirement has not been met. In the absence of federal regulation of birth certificates, the security in some individual states is very low, and there are many counterfeit or altered birth certificates in use as "breeder documents" for fraudulent identities. Under a grant by the Department of Transportation, a system which provides for electronic verification of birth certificates is now being operated in a pilot program by the National Association for Public Health Statistics and Information (NAPHSIS) and the American Association of Motor Vehicle Administrators (AAMVA). Federal funding is

needed to move this pilot program into a permanent system available to all states, but the cost is reasonable, probably in the range of $5 to $10 million per year.

**More Secure Social Security Cards**

Section 7213 requires the Commissioner of Social Security to: (1) issue regulations restricting the issuance of multiple replacement social security cards; (2) establish minimum standards for the verification of records supporting an application for an original social security card; and (3) add death and fraud indicators to the social security number verification system. The Commissioner is required to establish an interagency task force which is to set requirements for security improvements for social security cards and numbers.

Comment: This is a very important exercise. Regrettably, until the Social Security Administration is required by specific laws to improve the physical security of the card, to authenticate people's identities before issuing initial or replacement cards, and to set strict deadlines for both sets of requirements, there will likely be no meaningful security improvements by this important source of identity documents.

**Restrict the Use of Social Security Numbers on Cards**

Section 7214 amends Title II (Old-Age, Survivors and Disability Insurance) of the Social Security Act to prohibit the display of social security numbers on driver's licenses, motor vehicle registrations, or personal identification cards, or the inclusion of such numbers in a magnetic strip, bar code, or other means of communication on such documents.

Comment: States have largely changed their regulations and procedures to eliminate this practice, but it will be years before those issued prior to the Act will expire and be removed from circulation.

**Longer Sentences for Terrorist Identity Fraud**

Section 7216 amends the Federal criminal code to increase penalties for fraud and related activity in connection with identification documents and information if committed to facilitate international terrorism.

Comment: This law is specifically directed at terrorist support networks in the United States.

**Requiring Reliable Identification Documents to Board Commercial Airlines**

Section 7220 requires DHS to propose minimum standards for identification documents required of domestic commercial airline passengers for boarding. However, standards proposed take effect only when an approval resolution is passed by the House and Senate under specified procedures and becomes law.

Comment: This law remains in limbo because the Administration has not moved forward to establish standards. Until a set of standards, together with a set of procedures, is moved through Congress with an approving resolution, this common sense safeguard is not in place. Every time I move through security inspections at an airport, I am reminded that the inspectors have no real means available to authenticate the document that I present them. Very few airport security inspectors are trained to detect a fraudulent ID card. Nor are inspectors trained to detect and reject an altered ID card. Nor are inspectors yet authorized to reject as insecure a widely counterfeited ID card, such as the Matricula Consular card issued by the Government of Mexico or the driver's licenses of some of the states.

**REAL ID Act – Driver's License /Identity Document Provisions**

This law is not yet in effect, with the implementing Notice of Proposed Rule Making released March 1, 2007, and comments from public due by May 8, 2007. It is likely the implementing regulations will become final by the end of September 2007.

The REAL ID Act requires that a REAL ID driver's license be used for "official purposes," as defined by DHS.

In the proposed rule, DHS will limit the official purposes of a REAL ID license to those listed by Congress in the law: Accessing a Federal facility, boarding Federally-regulated commercial aircraft, and entering nuclear power plants.

DHS has set minimum standards for what will appear on the face of the card. The proposed regulation requires each of the following on the face of REAL IDs: (1) Space available for 39 characters for full legal name; (2) address of principal residence; (3) digital photograph; (4) gender; (5) date of birth; (6) signature, document number; and (7) machine readable technology.

Temporary REAL IDs will need to clearly state that they are temporary.

Non-REAL IDs issued by compliant States must state on their face that they are not acceptable for Federal official purposes and be of a unique design or color that clearly distinguishes them from REAL ID licenses. The Notice of Proposed Rule Making does not require a State to collect fingerprints, iris images, or other biometric data in connection with obtaining a license.

At this stage of development, only a traditional image is required, so long as it captured with digital technology allowing it to be exchanged / authenticated with other states.

2 – D Barcode is required, and RFID Chips are not. The Machine Readable Technology specified in the NPRM is the 2-D barcode already used by 46 jurisdictions (45 States and the District of Columbia) and not used by five.

Comment: REAL ID will eventually change how licenses look, but the initial proposed rule does not specify precise designs or layouts of state issued licenses or a single common layout. Greater commonality of design would greatly reduce the complexity of physical inspection, aid in detecting counterfeit and altered documents, and reduce training expense. However, DHS is undoubtedly responding to its extensive consultation with the more security conscious among the states, who have a legitimate interest in minimizing cost and protecting existing production facilities. In the absence of at least a few common design elements, the use of card reading and authentication machines with sophisticated operating software will become a standard requirement for law enforcement, and hopefully, airport inspectors.