AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OCTOBER 2005 STATUTORY DEADLINE FOR VISA WAIVER PROGRAM COUNTRIES TO PRODUCE SECURE PASSPORTS: WHY IT MATTERS TO HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 21, 2005

Serial No. 109–23

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

20–711 PDF WASHINGTON : 2005

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

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

JOHN N. HOSTETTLER, Indiana, *Chairman*

STEVE KING, Iowa
LOUIE GOHMERT, Texas
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
JEFF FLAKE, Arizona
BOB INGLIS, South Carolina
DARRELL ISSA, California

SHEILA JACKSON LEE, Texas
HOWARD L. BERMAN, California
ZOE LOFGREN, California
LINDA T. SÁNCHEZ, California
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts

GEORGE FISHMAN, *Chief Counsel*
ART ARTHUR, *Counsel*
LUKE BELLOCCHI, *Full Committee Counsel*
CINDY BLACKSTON, *Professional Staff*
NOLAN RAPPAPORT, *Minority Counsel*

CONTENTS

APRIL 21, 2005

OPENING STATEMENT

Page

The Honorable John N. Hostettler, a Representative in Congress from the State of Indiana, and Chairman, Subcommittee on Immigration, Border Security, and Claims 1
The Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Immigration, Border Security, and Claims 3
The Honorable Dan Lungren, a Representative in Congress from the State of California 28
The Honorable Howard Berman, a Representative in Congress from the State of California 30
The Honorable Jeff Flake, a Representative in Congress from the State of Arizona 31
The Honorable Louie Gohmert, a Representative in Congress from the State of Texas 33
The Honorable Steve King, a Representative in Congress from the State of Iowa 34
The Honorable Maxine Waters, a Representative in Congress from the State of California 40

WITNESSES

Mr. Rudi Veestraeten, Director General for Consular Affairs, Belgian Ministry of Foreign Affairs
Oral Testimony 6
Prepared Statement 8
Ms. Elaine Dezenski, Acting Assistant Secretary for Policy and Planning, Border and Transportation Security Directors, U.S. Department of Homeland Security
Oral Testimony 11
Prepared Statement 12
Mr. Richard L. Skinner, Acting Inspector General, U.S. Department of Homeland Security
Oral Testimony 16
Prepared Statement 18
Mr. Joel F. Shaw, President and Chief Executive Officer, BioDentity Systems Corporation
Oral Testimony 21
Prepared Statement 22

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Response to Chairman Hostettler's Question posed to Ms. Elaine Dezenski at the hearing, submitted by the U.S. Department of Homeland Security 46
Prepared Statement of the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin and Chairman, House Judiciary Committee 46
Questions for the Record submitted to the U.S. Department of Homeland Security by Chairman John N. Hostettler 48

Page

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas 50
Letter from the Travel Business Roundtable, Travel Industry Association of America, and U.S. Chamber of Commerce, submitted by the Honorable Sheila Jackson Lee 52
Prepared Statement of the Honorable Maxine Waters, a Representative in Congress from the State of California 53
Prepared Statement of the Honorable Elton Gallegly, a Representative in Congress from the State of Califonia 54

OCTOBER 2005 STATUTORY DEADLINE FOR VISA WAIVER PROGRAM COUNTRIES TO PRODUCE SECURE PASSPORTS: WHY IT MATTERS TO HOMELAND SECURITY

THURSDAY, APRIL 21, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 1:09 p.m., in Room 2141, Rayburn House Office Building, the Honorable John H. Hostettler (Chair of the Subcommittee) presiding.

Mr. HOSTETTLER. Good afternoon. Today we meet to determine whether the Department of Homeland Security (DHS) is prepared to address the October 26, 2005, deadlines mandated by law that come into effect on that date with regard to countries in the Visa Waiver Program.

This program allows travelers from certain designated countries to come to the United States as temporary visitors for business or pleasure without having to obtain a non-immigrant visa. There are currently 27 countries participating, and it is estimated that as many as 20 million foreign visitors entered the U.S. under the program in 2004. Clearly, it is of great importance to the U.S. travel and tourism industry and to the 22 million Americans employed in that industry.

Since its creation in 1986, the program has greatly facilitated travel to the United States from program countries. Through reciprocal arrangements, the program also benefits American international travelers.

The Visa Waiver Program was established on the premise that nationals of participating countries pose little risk of being security threats or overstaying the period of their admittance. Rules for eligible countries include the security of the travel documents they issue, among others, which is evaluated by the U.S. Government to validate continued participation.

The presumption is, because of the evaluation by DHS of the respective country's management of its travel documents, there is no need for pre-screening by State Department consular officers abroad. Without the exemption provided by the Visa Waiver Program, the consular officers would need to review documents provided by a visa applicant and interview the applicant to determine whether he or she posed a danger or was likely to overstay.

This premise may have been true in years past. It is not the case today. In December 2004, a "Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," issued by the DHS Office of Inspector General (OIG), painted a rather frightening picture. The OIG report said that aliens using stolen passports have little reason to fear being caught, are usually admitted, and that has made only a small difference whether the stolen passports were posted in the lookout system. When the results of that report are combined with continuing revelations of stolen blank passports, such as the thousands stolen in France last year, it seems to me that Congress needs to look again at DHS' security management of the program.

The Enhanced Visa Security and Visa Entry Reform Act of 2002 levied a series of requirements and deadlines to address the threats from terrorism from visitors entering as tourists and foreign students. Among these, it requires that by no later than October 26, 2004, the governments of Visa Waiver Program countries certify that they have programs to issue to their nationals machine-readable passports that are tamper-resistant and that incorporate biometric identifiers that comply with biometric identifier standards established by the International Civil Aviation Organization (ICAO). On or after this date, any alien applying for admission under the program must present a passport that meets these standards, unless the passport was issued prior to the date.

Last year, Congress acted to extend that important deadline for 1 year, in response to a request from the Administration, and promises by the Secretary of Homeland Security to strengthen inspections of visa waiver country programs for strengthening passport security.

This requirement would allow DHS inspectors at ports of entry to determine whether a passport properly identifies its bearer. This will combat terrorist imposters and prevent them from defeating lookout lists on which they are posted. Second, it will make passports harder to alter or counterfeit. Third, in conjunction with the planned installation of scanners at ports of entry to read the passports, DHS can track the arrival and departure of travelers and identify those who overstay their visas.

I would like to clarify for the record that the Border Security Act of 2002 required only that Visa Waiver Program countries issue passports for which the biometric identifiers and document security standards met ICAO standards and that were machine-readable. There was no requirement for a chip to be placed in a passport or in a visa in that Act. Nor did the legislative history nor any subsequent action by the Committee on the Judiciary or any part of the body of Congress call for a chip to become an integral part of the travel document security required for Visa Waiver Program countries. The act addressed the machine-readable ICAO standards that were in place at the time of passage in 2002.

The "chip standards" referred to in newspaper accounts which are effecting the delay are those established by the European Union, to apply to its member countries. If a visa waiver country decides to employ a chip as a security improvement to confirm identity, then the law requires it to comply with ICAO standards,

but it is not currently a requirement of U.S. law or of published U.S. Government rules of the program.

Once the chip technology is refined and becomes a reliable and proven means to improve passport security, it will be a useful and welcome tool for port of entry inspections. But a chip is not essential to enforcing the requirement established by Congress. The Border Security Act required only a biometric identifier and document security that met, once again, current ICAO standards at that time. The European Union's efforts to improve security are laudable, but the deadline is important to assure the public that we're serious about border security and about protecting against future terrorist attacks potentially launched from Europe.

Belgium has been issuing a viable passport since 2004 that appears to fully comply with the act's requirements. Our first witness today will provide us with the details of Belgium's success story.

The U.S. needs to establish specific and unambiguous requirements for biometric identifiers on travel documents presented by foreign governments in the Visa Waiver Program. It is the responsibility of the Department of Homeland Security to set those requirements and notify Visa Waiver Program countries what it is we will expect of them on October 26 of this year.

Mr. HOSTETTLER. At this time I turn and recognize the gentlelady from Texas, the Ranking Member of the Subcommittee.

Ms. JACKSON LEE. I thank the Chairman for holding this hearing sufficiently in time that we can have a collective and reasoned voice on this question, and hopefully we will have sufficient insight from the witnesses to recognize that although we have a responsibility for homeland security in this Subcommittee as it relates to our responsibilities and benefit, we also have the responsibility, I think, to keep an open understanding of the non-immigrant program, which includes the Visa Waiver Program, and at the same time we can acknowledge that we have made some steps of success toward securing the homeland. Therefore, this should allow us, although we're not perfect, to have some latitude, some reason to the expectation that all of the countries that are presently in the Visa Waiver Program will meet the necessary deadline, but at the same time that we would wish to deny them that right, longstanding allies and friends, simply because we were not willing to extend a deadline.

The Visa Waiver Program allows nationals from 27 countries to enter the United States as non-immigrant visitors for business or pleasure without first obtaining a visa from a United States consular office. This facilitates international travel and commerce and caseloads in consular offices. The Enhanced Border Security and Visa Entry Reform Act of 2002 mandated that by October 26, 2004, the Government of each VWP country would have to certify that it had established a program to issue machine-readable passports that are tamper-resistant and incorporate a biometric identifier.

We extended that deadline to October 26, 2005, last year. I think we were frugal and cautious by extending it by just a year, not necessarily determining that it would take only a year for them to complete their task and their assignment. The extension was necessary to avoid potential disruption of international travel and to

provide the international community adequate time to develop viable programs for producing a biometrically enabled passport.

According to the State Department, only 14 of the 27 VWP countries expect to comply with the revised deadline. Brunei, Finland, Ireland, Portugal, Spain, Switzerland, and the United Kingdom expect to come into compliance several months after the deadline. Long delays are expected by France, Japan, Denmark, Italy, Liechtenstein, and the Netherlands. Most of the countries that expect to meet the deadline are small countries that have small passport production numbers and centralized production processes. Hooray for them. Those with large passport production numbers are the ones who have the greatest difficulty in meeting the deadline. Many of them, for those who recognized some of the needs in Iraq early on, did coalesce with this nation in Iraq. The countries include France, Japan, Germany, and the United Kingdom, make up more than 80 percent of the VWP travelers, and as we well know, the United Kingdom, Great Britain, was an ally in the war in Iraq.

If the deadline is not extended, the VWP countries that fail to meet it will lose the privilege of participating in the program, and the nationals of those countries will need visas to enter the United States. The State Department has estimated that this would result in a sudden need to process millions of additional visas which would impose a severe challenge on its resources. I am concerned about the effect that even a temporary disruption of the Visa Waiver Program would have on the international tourist industry. In 2002, approximately 13 million international visitors entered the United States on the Visa Waiver Program. They spent nearly $40 billion and supported the jobs of hundreds of thousands of American workers. A disruption to the Visa Waiver Program would discourage international visitors. Many of them would choose to travel to other international destinations.

I am particularly concerned about the effect that this might have on the State of Texas. In the year 2000, Texas received revenue from the international tourist industry that totaled $3,751.3 million. This included $410.6 million in public transportation that was $3 billion, $111 million on automobile transportation, $1 million on lodging, and $731 million on—$1 billion on lodging and $731 million on food services, 320 on entertainment and general trade.

Also, the technology for the biometric feature needs to be fully developed and tested before it is put into use. I am afraid that rushing the VWP countries into compliance could result in passports that have unreliable biometric identifiers which will not provide the expected increase.

Mr. Chairman, I think it is important that we hold this hearing. I think it is important that we make the statement that we are serious. It is equally important that we void or make prohibitive the ability for terrorists to come on our soil. That is the first line of defense. It is also important that we have balance, recognize our allies, and work with our allies to ensure that they participate in this very important program.

As you well know, we have implemented the US-VISIT program that collects fingerprints electronically and compares individuals to a U.S.—to a watch list. The Advanced Passenger Information System provides information on international visitors before they ar-

rive, and these efforts are augmented by United States law enforcement and intelligence operations. Nevertheless, I want the biometric requirement to be met as soon as possible. I would only hope that we would extend or look at extending these in a reasonable fashion, that we will listen to the witnesses as they provide us insight on this very, very important question. Security is important, and we must do so in the current atmosphere of the 21st century with a number of our allies and those who have been part of the exchange in the United States in a fair and admirable way.

With that, I yield back.

Mr. HOSTETTLER. I thank the gentlelady.

Without objection, all Members' statements, opening statements, will be made a part of the record, including an opening statement by the Chairman of the Full Committee, Mr. Sensenbrenner, who had wanted to be here today, but his schedule overtook him, and he most definitely regrets not being able to make it. This is an issue that is of tremendous importance to the Chairman personally and was the subject of an extensive hearing in the recent past in the Full Committee.

Mr. HOSTETTLER. At this time I would like to introduce the members of our panel.

Rudi Veestraeten was appointed Director General for Consular Affairs, Belgian Ministry of Foreign Affairs, on December 20, 2002. Before taking up his new position, Mr. Veestraeten served in Belgian diplomatic missions in Niamey, Sofia, Bangkok, Nairobi, and Washington, D.C. He also held the position of Advisor to the Belgian Minister of Foreign Affairs between 1997 and 1999. Mr. Veestraeten has successfully reorganized Belgian passport issuance to improve its security. In fact, Belgium obtained the 2003 Interpol award for the best and most secure passport in the world. Mr. Veestraeten schooled in Roman languages at the University of Leuven in Belgium, and his wife, Mireille, and their two daughters live with him in Ulbeek, Belgium. Welcome, Mr. Veestraeten.

On March 4, 2005, Elaine Dezenski was appointed Acting Assistant Secretary for Policy and Planning within the Border and Transportation Security Directorate, U.S. Department of Homeland Security. Ms. Dezenski joined BTS from the Transportation Security Administration. Prior to joining the TSA, Ms. Dezenski served as a special assistant to the Administrator of the Federal Transit Administration. Ms. Dezenski also served as a Brookings Institution LEGIS fellow for Congressman Sherwood Boehlert. She holds a master's degree in public policy from Georgetown University and a bachelor's degree in international relations from Wheaton College, Norton, Massachusetts.

Richard Skinner is the Acting Inspector General at the Department of Homeland Security. He has also served as the Acting Inspector General at the Federal Emergency Management Agency. Mr. Skinner went to FEMA in 1991 from the U.S. Department of State where he served as the Inspector General's representative to the Arms Control and Disarmament Agency. Prior to that, Mr. Skinner managed the Inspector General's International Trade Division at the U.S. Department of Commerce. Mr. Skinner holds a B.S. degree in business administration with an MPA degree from George Washington University.

Joel F. Shaw is President and CEO of BioDentity Systems Corporation. He is a recognized expert in the fields of official documents of identity, related technology systems, and border clearance systems. Mr. Shaw is the convener of the International Standards Organization Working Group responsible for development and maintenance of Standards for Machine Readable Travel Documents. He also coordinates and provides ISO's liaison with the International Civil Aviation Organization.

Will the witnesses please rise to take the oath?

[Witnesses sworn.]

Mr. HOSTETTLER. Thank you. You may be seated.

Please let the record reflect that the witnesses responded in the affirmative.

Mr. Veestraeten, please begin your testimony. We have a light system that is for a total of about 5 minutes. Your entire written statement will be made a part of the record. We very much appreciate your presence here today and look forward to your testimony.

TESTIMONY OF RUDI VEESTRAETEN, DIRECTOR GENERAL FOR CONSULAR AFFAIRS, BELGIAN MINISTRY OF FOREIGN AFFAIRS

Mr. VEESTRAETEN. Mr. Chairman, Ranking Member Jackson Lee, and distinguished Members of the Subcommittee, I want to thank you for giving me the occasion to testify before this Subcommittee. I presume that I have been invited because today Belgium is the first and the only country which completed the rollout of an ICAO-compliant electronic passport. I would like to share with you our views and achievements.

I'm going to make some comments as a complement to the notes I deposited earlier. I would like to apologize for any linguistic flaws in my wording, both in the notes and before the esteemed Subcommittee. Although I had the honor and the pleasure to serve here in Washington, D.C., I never really achieved the level of fluency and accuracy, but my daughters did while staying here a couple of years ago.

However, I would very much like to highlight some aspects of the Belgian achievements in the field of passport security. I truly believe we did a good job as a middle-sized country, and even better securing our national passports, after we received the Interpol award for having realized the world's best passport in 2003. This was, to be precise, sometime before we decided to take our national travel document a step further and to include the new technology of the computer chip into the already fine passport.

First of all, I would like to refer to the note regarding our passports, which includes technical specifications. We wanted a solid solution, surviving genuine Belgian travelers' behavior, and I'm confident Belgians don't behave better or worse than other citizens. So we developed tests, including chemical exposures to set a new standard. Our passport passed all of these tests, of course.

Secondly, we did not only deploy a passport but also passport readers, not only classical readers you plug into a computer, but also a new, affordable, mobile reader. I believe our approach based on an off-the-shelf solution is also innovative.

The Belgian federal police, in charge of border control, already deployed these readers in the Brussels airport, in the port of Antwerp, and we are, of course, very much willing to share our experience in this field with all the partners. I had several meetings this week with my American colleagues in this regard.

In the third place, I want to stress how much we want to make sure that new high-tech passports do not fall in the hands of the wrong persons. Belgium has developed over the past decennium a quite unique system of registration of its citizens. When I had the honor to serve in your country some years ago, I appeared before this Congress' standing Committee on Citizenship and Immigration on November 16, 2001, to testify about the national identity cards and the Belgian registration process of citizens. You might find it useful to consult that information, which is still valid today. The system has not changed since then.

Finally, and not least, I also wanted to make sure that lost and stolen passport information is readily available to all concerned. This is why we developed a new approach to this problem. We published an Internet-based consultation tool. You can now check a given Belgian passport number against a daily updated list of stolen and lost documents and learn whether it has been reported stolen or lost or not. Nothing more, nothing less.

I brought a fresh text today to this meeting on this new tool. The tool is still experimental, and this tool might be improved after input by our partners.

We also offer a so-called web service to this—to our international partners to this tool, which means that others, like U.S. Immigration, can automate the consultation of this online list of lost and stolen passports. This new approach has been very well received by my American colleagues this week, and we are also willing to share this with all countries which are interested.

Five minutes, Mr. Chairman, is not a long time, especially for a complex issue like passport security. I hope I made it clear that all the aspects I mentioned above are equally important and that my country has gone a long way to address them all. We did not just put a chip in the passport. We did a lot more.

Now, Belgium is not alone in this, and it is a bit odd to see that we already have today around 170,000 ePassports in circulation, the number growing by 40,000 each month, and by the end of this year, Belgium alone will already have more than half a million passports with a chip in circulation. Currently, no country, except Belgium itself, has deployed ePassport readers. Of course, it is essential that we all build the capacity to read the chip.

Belgium is not alone, I said. I am wearing a special tie today, a necktie, the tie of the Luxembourg Presidency of the European Union. Let it be the symbol of this message: that I truly believe that only an inclusive approach in which all well-meaning countries are involved and accepted can lead to better travel and passport security. With the authority of my achievements, I want to plead for inclusion and not for exclusion. It is not a good policy to leave countries out. We all face the same difficulties and challenges in Europe and outside Europe, and we can surely learn from each other.

I want to conclude on this, an appeal for inclusiveness, for continued high standards for security, and for close cooperation between all countries involved.

I want to thank you, Mr. Chairman, esteemed Members of the Committee, for this occasion to speak out.

[The prepared statement of Mr. Veestraeten follows:]

PREPARED STATEMENT OF RUDI VEESTRAETEN

The Belgian ePassport, part of an integrated security approach

Belgian ePassport production launched November 15, 2004

Belgium is the ***first country worldwide*** to complete its roll out of ICAO-compliant electronic passports (ePassports). The achievement means it meets both US and European deadlines for the implementation of biometric-based ePassports, which pass on 26 October 2005 and June 2006 respectively.

After pilot tests earlier in 2004, production started on November 15 last year, with 10% of total passport production being ePassports. Production was ramped up by a further 10% each week over a 10-week period. Since ***January 30, 2005*** all new passports issued contain contactless chip technology.

The gradual roll out ensured a smooth transition to chip integration in all new passports. In total, ***150,000 ePassports*** have been produced to date.

Technical specifications

The passport chip contains 72K of memory, of which 64K is available. This allows it to flawlessly store all the information already printed on the data page of the passport. These data are : the name, first name, date and place of birth, the passport number, issuing date and place, and a ***digital photo***. This is in full compliance with the current European and US standards. As and when international standards are further developed, the same chip will also be able to store other biometric information such as the fingerprint (the EU deadline for the implementation of another biometric feature in the passport is December 2007).

The contactless chip is located in the back cover of the passport and is activated via a serigraphic (printed) antenna. This design of antenna is ***very flexible***, helping to ensure the durability of the passport design during its five-year life. Earlier tests with an unflexible design had failed.

In the 1990s Belgium had experienced problems with passport falsification. However, the implementation of a centralised distribution network and other technical innovations led to the Belgian Passport receiving "the world's most secure passport" ***award*** from ***Interpol*** in 2003. Specific security features included a laser micro perforated negative of the of the picture, holograms, the multicolor image laminate under UV light and special high-tech inks and printing techniques. A special page indicates these security features to help

foreign police and border-inspectors to distinguish immediately an authentic from a false passport. All of these innovations taken together make the Belgian passport very tamper resistant.

The technical solution of a flexible incorporation of the computer chip has been thoroughly ***tested*** in a high-tech ***laboratory***. Tests such as long-term exposure to high and low temperatures, to a torsion and a chisel-test ('Ikea-style' testing), chemical tests (both solvents such as diethylene glycol, ethyl acetate, ethanol, ethyl ether, toluene, tetrachloroethylene, petroleum ether; and acids & bases such as sulfuric acid, hydrochloric acid, acetic acid, sodium bicarbonate, ammonia aqua, sodium hydroxyde and sodium hypochlorite) have been applied to the newly developed passport before launching.

No standards for such testing have yet been established internationally, and Belgium has suggested to ICAO that the specific tests developed nationally be adopted by the international organization in order to further enhance the deployment of this new technology by the world community.

Belgian ePassport: an integrated solution

The new Belgian ePassport is not a stand-alone solution. In close cooperation with the ***Belgian Federal Police force***, in charge of border control, Belgium is also the first country worldwide to roll out systematic check of ePassports.

Foreign Affairs in Belgium have also been actively developing both USB-style ePassport readers and low-cost ***mobile ePassport readers***.

USB-readers are not an innovation: they are readily available and allow for immigration officers to check passport chips at entry gates. Belgium wanted to develop a mobile reader, making it possible for immigration or police officers to check an ePassport in all conditions: at an airport gate, for random checks in the airport area or even during patrolling in town.

The Belgian solution is based on a standard PDA (Pocket PC), with a dedicated antenna connected via one of the device's memory slots. The PDA is able to authenticate the passport, check the passport against a previously downloaded list of stolen documents and display the content of the chip, including an enlarged image of the facial image on the screen. The entire process takes 6-8 seconds and the cost of the reader is in the region of $500 - $600. There is also space for future developments, such as the addition of a fingerprint sensor if needed.

In the view of the Belgian authorities, the broad deployment and easy access for police officers of ePassport readers is essential to the successful adoption of the new technology. This is the main reason why Belgium has spent so much energy on the mobile reader's development and deployment.

The latest development includes an online website www.diplomatie.be/passweb on which the status of a Belgian passport can be verified. This website is linked to a centralized electronic database of stolen and lost passports that is accessible by every authority or even private person.

Passport issuance: a national concern

A said before, the ePassport is not a stand-alone solution. It is essentially part of a renewed, integrated security concern. This is why verification of passport applicant's identity is of the utmost importance.

Identity theft is, unfortunately, a widespread phenomenon in many countries but not in Belgium. All citizens are registered with an address by the local authorities, and all registration information is available in a centralized database.

Identity security is guaranteed by ***the triple verification*** of the decentralized individual paper file, of the decentralized registers of civil certificates and of the mandatory registration in the centralized electronic database "the national register". Each Belgian worldwide has since his birth such a triple file.

Please be assured: the information stored in that database is very secure, and is only available to the specifically authorized authorities. All consultations of these files are properly logged.
Belgium has a very severe privacy legislation. High penalties including prison sentences are strictly applied in case of abuse. Moreover, every citizen can see online who looked into his or her file, and if need be file a complaint.

The passport issuance procedure is based upon this registration. One can only apply for a passport at the location of one's registration, where the local authority has access to the complete file, including previous application forms and pictures.

This makes it impossible to steal another persons identity and obtain a authent ly secured passport in that other person's name.

Belgium ecently launched ***an electronic identity card*** (eID). This is the newest generation of the Belgian identity card which has been issued since 1865. Our country had the occasion to inform the US Senate about the history and practice of the Belgian national identifier in the year 2002. The recent step-up of this card, now with an electronic chip, was welcomed by the security world community as well as by the industry. Both Microsoft and Adobe have announced the future integration of the Belgian eID in their computer software.

Washington, April 20, 2005.

Mr. HOSTETTLER. Thank you, Mr. Veestraeten.
Ms. Dezenski.

TESTIMONY OF ELAINE DEZENSKI, ACTING ASSISTANT SECRETARY FOR POLICY AND PLANNING, BORDER AND TRANSPORTATION SECURITY DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. DEZENSKI. Thank you, Mr. Chairman, Ranking Member Jackson Lee. I appreciate the opportunity to be here today. I'm going to talk a little bit in my oral remarks about combating illegal travel with a specific focus on lost and stolen passports, and we'll get to a nexus with VWP as well.

First I'd like to request that my written testimony be submitted for the record. Thank you.

Mr. HOSTETTLER. Without objection.

Ms. DEZENSKI. Thank you.

Let me start by talking about the layered solution. DHS, in cooperation with the Department of State, and many of our international partners rely on a layered strategy to combat the threats of illegal travel, most significantly, of course, terrorist travel. In the air and sea environments, our approach to this problem begins well before a foreign national arrives in the U.S. through the transmission of advanced passenger information, and it continues as travelers seek admission at the border. It is completed upon exit where many foreign nationals are or will soon be subject to biometric exit procedures under the US-VISIT program.

At the land border, we are completing implementation of US-VISIT entry capabilities, implementing additional systems to verify a person's identity, exploring the use of technologies to automatically capture arrival and departure information, and we are developing new documentation requirements as part of our Western Hemisphere Travel Document Initiative. So there are many layers to this approach.

Within this layered solution, we have also worked diligently to implement each of the IG's recommendations from its 2004 report on lost and stolen passports. Since the completion of that audit, DHS has taken action on each of those recommendations—there were eight—and all are now considered either closed or otherwise resolved. As a result of this effort, today when State or DHS receives information on lost or stolen passports, that information is entered into our lookout systems within 72 hours, but normally much faster than that. Information is primarily entered by State into their system called CLASS, or the Consular Lookout and Support System, and electronically transferred within an hour to the DHS Interagency Border Inspection System, or IBIS, which is at all of our ports of entry.

Several actions can then take place. Our border inspectors have access to this information through IBIS at the primary inspection point. When we find a match that individual is given a mandatory secondary inspection. Those who attempt, knowingly or otherwise, to enter with a lost or stolen passport are not admitted to this country, no exceptions. And the false passport is confiscated and sent to CBP, to our new fraudulent document analysis. Again, no exceptions.

In addition, the National Targeting Center will analyze this information to ensure that no one has already entered on that lost or stolen document. If we find that someone was admitted prior to our knowledge of that lost or stolen piece of information, the Investigation and Customs Enforcement Directorate initiates their investigation process immediately. And for all cases where we have a lost or stolen passport and there's potential of link to terrorist activity, we refer that case to the U.S. Attorney for prosecution.

In order for the system to work, we need to obtain data from our international partners. State and DHS rely on dual reporting regimes to ensure that we obtain that type of information in a timely manner. First, we work with the international community to promote universal reporting of lost and stolen passports through the Interpol Lost and Stolen Document Database, thereby centralizing the way that that information is handled. To date, the U.S. has provided over 500,000 such records on our lost and stolen data. We've excluded personal information for the holder, but have provided that information to help build that database. And we've obtained agreement from our G–8 partners to utilize the database for their information as well.

In addition, statute now requires Visa Waiver Program countries to report lost and stolen blank passport information to us in a more timely manner. This requirement is in addition to the mandate that these countries begin issuing biometric passports by October 26, 2005. While scientific and technical challenges have contributed to slowing the implementation of the biometric requirements, we have received significant cooperation and moved forward on lost and stolen passport reporting issue. How a VWP country continues to handle this important responsibility is a critical test in our determination if a country should remain eligible for the program.

DHS has recently concluded its review of the VWP program as mandated by the Enhanced Border Security and Visa Entry Reform Act of 2002, and a draft report to Congress is being prepared and finalized for transmission to the Hill. We look forward to briefing you further on this important effort once that report is cleared.

As Secretaries Ridge and Powell indicated in their testimony last year, a clearly stated goal of the international community is to establish an integrated chip in the passport to verify both the biometric identifier and validity. DHS and State remain committed to this goal and more broadly to pursuing the best possible biometric solutions that can be adopted and utilized on an international basis.

By implementing the IG's recommendations, improving our access and use of data, and strengthening the security features of the passport, we are creating important obstacles to terrorists and criminals who seek to circumvent our border control efforts. Many challenges remain, but we look forward to working with the Committee to ensure robust solutions are implemented as soon as practical.

Thank you.

[The prepared statement of Ms. Dezenski follows:]

PREPARED STATEMENT OF ELAINE DEZENSKI

Chairman Hostettler and Ranking Member Jackson Lee and other distinguished Members, it is a pleasure to appear before you today to discuss the actions that the Department of Homeland Security (DHS) has taken to address the issue of the use

of lost or stolen passports for illegal travel to the United States and minimize, if not eliminate, related security risks. I will also provide an overview of the steps taken to enhance the security of the Visa Waiver Program.

DHS has taken a variety of actions to address concerns raised by the DHS Office of the Inspector General in its 2004 Report, specifically regarding the functions of the National Targeting Center (NTC), our efforts to detect fraudulent travel documents, and our US-VISIT biometric screening system which helps to "fix" the identities of individuals entering and departing the United States by capturing biometric information at the time of inspection, comparing it to any biometric identification information previously collected during the visa issuance process and confirming it upon departure, when possible, through US-VISIT.

LAYERED SECURITY

DHS and DOS together have created a continuum of security measures that begins before individuals enter the United States. Identity verification measures begin overseas and continue upon entry and exit from this country. This layered system, described below, includes the secure storage of biometric and biographic data and uses travel and identity documents to access that information for identity verification and watchlist checks.

Advance Passenger Information (API) data transmitted by air carriers and cruise ships is queried against the lookout databases at the NTC prior to the travelers' arrival in the United States. The NTC has access to additional information to assist in the analysis of the API and identify potential lookout subjects, holders of passports reported as lost or stolen, criminals, and other immigration violators. In addition, biometric and biographic information is also checked against various databases linked under US-VISIT which contain visa issuance information, terrorist (through the Terrorist Screening Database (TSDB) and criminal watchlists, and immigration status information through US-VISIT. That information allows a Customs and Border Protection (CBP) Officer at the border to verify the identity of the traveler and check terrorist, criminal, and immigration violator watchlists.

Since January 5, 2004, 20.5 million entries have been recorded through US-VISIT and 471 criminals and immigration violators have been denied entry based on biometric information. On September 30, 2004, we began enrolling nationals from Visa Waiver Program (VWP) countries in US-VISIT when they travel to the United States and on December 29, 2004, US-VISIT was rolled out to the 50 busiest land border ports of entry.

We are also reviewing how travel documents are produced and reviewed by foreign governments so that Consular Officers at embassies and consulates and Border Inspectors at the ports of entry can better detect altered and counterfeit documents, improve and expand watch lists and how they are vetted, and explore ways to share data with our counterparts that can help identify and thwart those attempting to use such documents to enter the United States illegally, particularly terrorists. Additionally, we continue to promote appropriate security and privacy controls to protect the information contained within our databases and on the travel documents we issue.

LOST AND STOLEN PASSPORT DATA

DHS, in cooperation with the Department of State (DOS), international organizations and our allies abroad, is making strides to address the issue of lost and stolen passports. First, here at home, as information on lost and stolen foreign passports becomes available, DOS and DHS' CBP personnel officers enter this information into the government's lookout systems within 72 hours, as required by the Enhanced Border Security and Visa Entry Reform Act (EBSA) of 2002. CBP incorporates lost and stolen passport information into its systems to aid in the detection and interception of persons using lost and stolen documents.

Second, across the globe, we are making headway in our efforts to encourage governments to collect and share data on lost or stolen passports. International border control authorities traditionally seek timely and accurate information concerning the validity of travel documents presented at embassies and consulates and at ports of entry. In most cases, countries are able to recognize the misuse of their own documents. However, because of concerns about the use of personal data, many nations have been reluctant to share data on lost or stolen travel documents with other governments or international agencies. Through the efforts of the DOS and the Department of Justice, the United States has taken the lead in providing information on lost and stolen passports, with over 500,000 records of lost and stolen passports provided to the Interpol's lost and stolen document database, which is available to border authorities worldwide. Many other countries are doing the same and efforts are

under way internationally to enhance such exchanges of information. At the June 2004 G8 Summit, G8 partners agreed to a U.S. proposal to start providing information on lost and stolen passports to the Interpol database by December 2004. Some European Union countries have started providing comprehensive information on lost and stolen passports to Interpol. We want to advance this effort beyond the G8 and encourage all countries to submit relevant information to the Interpol database. We are promoting a comparable initiative among the APEC economies to develop a Regional Movement Alert System.

Similarly, on a bilateral basis, we worked with our colleagues at DOS to exchange information with the Government of Australia on lost and stolen passports. A bilateral agreement—the first of its kind—was just signed to allow bilateral exchange of lost and stolen passport information.

DETERRING THE USE OF FRAUDULENT DOCUMENTS

In the border and immigration enforcement arenas, biometric identifiers are tools that help prevent the use of fraudulent identities and travel documents. The purpose of the biometric identifier is to verify a person's identity in order to run his/her information against Terrorist Lookout or Watchlist data, to do a criminal history check against extracts from the FBI's IAFIS system and to ensure that an individual cannot apply and/or be granted benefits under an assumed identity. Biometric visas issued by the DOS to travelers to the United States allow one-to-one matches, to verify that the person presenting the visa is the person who was issued the visa, and one-to-many matches, to ensure that the bearer is not the subject of a biometric lookout or enrolled in the system under another name. Like the biometric visa process at time of visa issuance, US-VISIT enrollment "fixes" a person's identity at the port of entry. When a VWP traveler enrolls in US-VISIT, the person's fingerprints are electronically linked to the passport in the US-VISIT database thus preventing another person from fraudulently using that passport at a port of entry with US VISIT by freezing identities at the border and ensuring that the person is not enrolled under another name.

While advances in technology allow our dedicated and hardworking CBP Officers to examine and validate documents presented for reentry, that same technology also enables the perpetrators of fraud to produce, relatively inexpensively, high-quality fraudulent documents. Forgers and counterfeiters can produce high-quality fake birth certificates and driver's licenses with off-the-shelf software programs and materials that are difficult to detect without sensitive instruments and sufficient time to examine them.

Our CBP Officers are also charged with detecting look-a-likes or impostors who attempt to use valid documents which belong to another person. This is one of the fastest growing phenomena in travel document abuse. Document vendors solicit genuine, unaltered documents and match them up with "look-a-likes." DHS' Immigration and Customs Enforcement (ICE) has developed a training program to detect impostor documents, which it has conducted for both U.S. and foreign immigration and border officers around the world.

NATIONAL TARGETING CENTER

The NTC is primarily staffed by CBP. The NTC staff consists of CBP Officers and field analysis specialists who are experts in passenger and cargo targeting for air, sea, and land operations in the inbound and outbound environments. The NTC develops tactical targets—potentially high-risk people and shipments that should be subject to additional scrutiny by CBP personnel—and it develops these targets from raw intelligence, trade, travel, and law enforcement data.

The NTC has access to over 20 critical anti-terrorism, border security and law enforcement databases, including the Terrorist Screening Data Base (TSDB) maintained by the Terrorist Screening Center (TSC), and receives strategic intelligence daily from CBP's Office of Intelligence, our IAIP Directorate, and other law enforcement and intelligence entities. The NTC includes representatives from ICE, the FBI, the intelligence community, the Transportation Security Administration (TSA), US-VISIT, the Department of Energy, the Department of Agriculture, the Food and Drug Administration, and the United States Coast Guard.

NTC supports DHS field elements, here and overseas, including the Visa Security Program, and the Immigration Advisory Program, currently operating at Schiphol Airport in Amsterdam and Warsaw, Poland, where teams of CBP officers are deployed to work with local authorities in preventing the onward movement of people identified as attempting to travel using fraudulent documents or presenting a security threat to the carrier or passengers on international flights destined to the U.S CBP Officers at all of our ports of entry,.

During the period of heightened alert in December 2003, the NTC played a pivotal role in analyzing advanced passenger information system (APIS) manifests related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

DHS is committed to improving the current collection of passenger manifest information over the coming months by standardizing entry information formats, requiring departure information, and finalizing crew manifest requirements.

The United States and the European Commission signed an international agreement on May 28, 2004 permitting DHS to access passenger name record (PNR) data to be used for screening passengers. PNR data is an essential tool allowing DHS to accomplish key goals. PNR data helps us make a determination of whether a passenger may pose a significant risk to the safety and security of the United States and to fellow passengers on a plane and PNR data is essential to terrorism and criminal investigations by allowing us to link information about known terrorists and serious criminals to co-conspirators and others involved in their plots, as well as to potential victims. Sometimes these links may be developed before a person's travel, but at other times these leads only become available days or weeks or months later. In short, PNR data helps DHS fulfill its anti-terrorism and law enforcement missions and allows for more efficient and timely facilitation of travel for the vast majority of legitimate travelers to and through the United States. At this time, CBP is receiving PNR data, which is enabling us to link information about known terrorists.

VISA WAIVER PROGRAM

The Visa Waiver Program (VWP) currently enables citizens of 27 countries to travel to the United States for tourism or business for ninety days or less without obtaining a visa. While the VWP encourages travel and trade, it is also an attractive means of entering the United States for those wishing to avoid visa-security checks conducted at U.S. consulates abroad. To mitigate the vulnerability posed by the misuse of the VWP as of September 30, 2004, DHS began to enroll VWP applicants in US-VISIT. This step narrowed security gaps by providing biometric watchlist checks and identity verification for subsequent visits to the United States.

By law, DHS, in consultation with DOS, is required to review all participating countries periodically for continued participation in the VWP and report to Congress. Several countries (Slovenia, Belgium, Italy, Portugal, Uruguay, and Argentina) were reviewed by the legacy Immigration and Naturalization Service (INS), and two (Argentina (2002) and Uruguay (2003)) were removed from the program. DHS, in coordination with the Department of State, is finalizing the current reviews for the remainder of the countries. This is the first comprehensive review of the countries and will form the "baseline" for future reviews.

In addition, as DHS and DOS conduct the required reviews of countries participating in the Visa Waiver Program, each country has provided detailed information about lost and stolen passports, their law enforcement response to such incidents, and efforts made to tighten distribution and document security processes. How a country handles this key issue will be an important factor in how DHS, working with interagency teams, determines whether VWP countries remain eligible for the program. These reviews are being finalized and the Report to Congress is being prepared.

The Enhanced Border Security and Visa Reform Act (EBSA) of 2002 required that, beginning on October 26, 2004, VWP countries each certify that they have a program in place to issue to their nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with International Civil Aviation Organization (ICAO) standards as a condition of continued participation in the VWP program. The law also required that visitors coming to the United States under the VWP present machine-readable, tamper-resistant passports that incorporate biometric and document authentication identifiers, if the passport is issued on or after October 26, 2004. Furthermore, DHS is required to install equipment and software at all ports of entry to allow biometric comparison and authentication of these passports. Prior to the October 26, 2004, deadline, and at the request of the Administration, Congress enacted an extension of the deadline for both VWP travelers to use biometric passports and for the U.S. Government to install the equipment to read the passports. The current extension deadline is October 26, 2005.

CONCLUSION

We have made much progress to deter the travel of individuals using fraudulent or stolen passports and other travel document and identify potential travel

facilitators. Our colleagues at DOS have also made great strides in developing new electronic passports that include internationally developed technology. In addition to the initiatives described above, we are working aggressively with our USG colleagues, and international partners to improve standards for travel documents, enhance aviation safety and port security, and speed the exchange of identifying information.

I would be happy to answer any questions you have at this time.

Mr. HOSTETTLER. Thank you, Ms. Dezenski.

Mr. Skinner.

TESTIMONY OF RICHARD L. SKINNER, ACTING INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SKINNER. Thank you, Mr. Chairman, Ranking Member——

Mr. HOSTETTLER. Could you push the button on your microphone?

Mr. SKINNER. Let's do that.

Mr. HOSTETTLER. Thank you.

Mr. SKINNER. Okay. Thank you. Mr. Chairman, Members of the Subcommittee, I'm pleased to be here today. I've provided the Subcommittee with a written statement for the record. I'll summarize it in these remarks, if I may.

In December 2004, our office issued an inspection report, "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States." The Visa Waiver Program began as a pilot program in 1986 and has evolved into a permanent program in which 27 nations participate. The program enables most citizens of these countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. From the beginning, the program involved the balancing of security risks and benefits to commerce, tourism, foreign relations, and the workload of the Department of State.

Virtually all of those familiar with the Visa Waiver Program told us that lost and stolen passports are the greatest security problem associated with the Visa Waiver Program. In response to these concerns, we examined all reported stolen passports from six visa waiver countries—France, Spain, Germany, Portugal, Belgium, and Italy—for a 5-year period, February '98 to February 2003. There were 3,987 reported passports stolen; some were presented 176 times at American ports of entry.

We concluded that our country was vulnerable because of gaps in our treatment of lost and stolen passports. To be specific, the Department did not have a process to check lost and stolen passport information against entry and exit information to determine the scope of fraud. Upon receipt of a new report that passports had been stolen, it did not check to determine whether they had been used already to enter the United States, nor did it have a formal procedure to notify the Bureau of Immigration and Customs Enforcement of the use of a stolen passport in order to facilitate an effort to apprehend the traveler.

Also, there continue to be problems with how the United States obtains lost and stolen passport information from visa waiver governments and the manner in which that information is collected. In at least one foreign country that we visited, there was uncertainty over how to report thefts of passports to the United States.

Even when lost and stolen passports were reported to the United States and entered into the U.S. lookout systems, they still may be used to enter through our ports of entry or to the U.S. It made little difference whether a passport had been listed in a lookout or not. Travelers using stolen passports that had not been posted to the lookout were admitted 81 percent of the time, 79 times out of 98 attempts. Travelers using passports that had been posted to the lookout were admitted 73 percent of the time, or 57 times out of 78 attempts. Thirty-three of these occurred after 9/11. Most disturbing, some came from stacks of stolen passports that were associated with events possibly linked to al Qaeda.

Some stolen passports were used multiple times to enter the U.S., even after being posted on the lookout system. Due to the limited data collected by inspectors at ports of entry, we were often unable to determine the inspector's rationale for having admitted the aliens.

We made seven recommendations to address the vulnerabilities that we noted. The Department agreed with each of our recommendations.

One of the most significant steps taken by the Department is the processing of visa waiver travelers through the US-VISIT program. This will permit additional screening, identification, and extra control features for all travelers from visa waiver countries.

A second and equally important concern was the ill-fated process by which information about a country's stolen and lost passports are reported and disseminated among other countries. We are, therefore, pleased to learn of the Interpol plan to consolidate and to report lost and stolen passports. This initiative should be of great benefit when fully implemented and when all nations participate.

Even with the completion of the corrective actions that we recommended, the Visa Waiver Program will always pose some security risk. The fundamental premise of the program is that millions of people, about whom we know very little, can be exempted from the more vigorous—or rigorous visa procedures and permitted to enter the United States. As we said in our Visa Waiver Program report—that was dated in—that was issued in April 2004, "The visa is more than a mere stamp in a passport. It is the end result of a rigorous screening process that the applicant must undergo before entering the United States." By the end of the U.S.—or by the end of the visa interview, the Department of State has collected and stored considerable information about the traveler and the traveler's planned journey. It has introduced biometric features into its visas, shares data from its visa records with our port of entry systems, and significantly increased the percentage of applicants subject to a careful interview. In contrast, the visa waiver traveler is interviewed briefly, and the passport examined, again briefly, by an inspector who may be—or may not be familiar with passports from the issuing country.

Mr. Chairman, this concludes my remarks. I'll be happy to answer any questions you or the Committee may have.

[The prepared statement of Mr. Skinner follows:]

PREPARED STATEMENT OF RICHARD L. SKINNER

Thank you, Mr. Chairman and members of the Subcommittee:

I'm pleased to have this opportunity to appear before you today to discuss the findings of our December 2004 review of the use of stolen passports from Visa Waiver countries to enter the United States and the threat that stolen Visa Waiver Program (VWP) passports pose to that program. More broadly, this is a threat posed to our national security as well. Copies of the report have been provided to the Subcommittee and are available to the public on our website.[1]

What did we inspect?

The VWP began in 1986. It enables most citizens from 27 countries to travel to the United States for tourism or business purposes for 90 days or less without obtaining a visa. From the beginning, the program involved a balancing of security risks and benefits to commerce, tourism, foreign relations, and the workload of the Department of State. In late 2003 and early 2004 we studied the security implications of the visa waiver program and released a report in April 2004. Copies of that report also have been provided to the Subcommittee and are available to the public on our website.[2]

Virtually all those familiar with the Visa Waiver Program told us at that time that the lost and stolen passport problem is the greatest security vulnerability associated with it. During the course of our VWP review we obtained documents that recorded instances in which blank, bona fide passports from VWP countries were stolen and, as determined from their serial numbers, later used to enter the United States, sometimes on multiple occasions. In some instances, entry was permitted even after the stolen passport had been posted in the lookout system. We therefore began a subsequent inspection of the specific problem posed by stolen VWP passports and issued a report in late December 2004.

What did the data show?

We examined all reported stolen passports from six VWP countries—France, Spain, Germany, Portugal, Belgium, and Italy—for a 5-year period—February 10, 1998, to February 12, 2003. There were 3,987 reported passports stolen; some were presented 176 times at Ports of Entry (POE).

Aliens applying for admission to the United States using stolen passports had little reason to fear being caught and usually were admitted, even if the stolen passport had been posted previously to CBP's lookout systems. Also, when DHS received new reports of stolen passports, it listed the passport number into its lookout system for future protection but did not check to determine whether a traveler had already used any of the newly reported passports. Finally, the Department of Homeland Security (DHS) did not have a sound procedure to ensure that when CBP records show a successful entry using a stolen passport, the event is referred to Immigration and Customs Enforcement (ICE) investigators to seek out and apprehend the user.

It made little difference whether the passport had been listed in a CBP lookout or not. Travelers using stolen passports, which had not been posted to the lookout, were admitted 81% of the time; travelers using stolen passports that had been posted to the lookout were admitted 73% of the time.

With respect to travelers whose passports had already been posted to a lookout as stolen, half were referred to "secondary inspection" for a more thorough examination. However, most referrals were for other reasons. The use of a stolen passport was not a recorded basis for the referral. Thus, after examination in secondary, half of the travelers were permitted entry. Some passports were used successfully multiple times to enter, despite being posted on the lookout system. We could not determine the inspectors' rationale for admitting the aliens with lookouts for the stolen passports. The records of the secondary inspections often were nonexistent or so sketchy that they were not useful.

Of the admissions on stolen passports, 33 occurred after September 11, 2001. Most disturbing, some passports that were used successfully came from blocks of stolen passports, which were associated with events or locations possibly linked to Al Qaeda.

DHS did not have a process to check lost and stolen passport information against entry and exit information. Upon receipt of a new report that passports have been stolen, CBP did not check to determine whether they have been used to enter the

[1] "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States" (OIG–05–07) December 2004.

[2] "An Evaluation of the Security Implications of the Visa Waiver Program" (OIG–04–26) April 2004.

United States, nor did it have formal procedures to notify ICE of the use of a stolen passport so that an effort may be initiated to apprehend the traveler.

We recommended that CBP:

1. Require inspectors to refer aliens to secondary inspections when the passports are the subjects of lookouts;
2. Require that inspectors record in detail the results of the secondary inspections and justifications for subsequent admissions;
3. Require that a supervisor review and approve an inspector's decision to admit an alien who was the subject of a lookout, and that the review be recorded as part of the secondary inspections record;
4. Initiate routine reviews of admission records to identify prior uses of stolen passports; and,
5. Report information on the successful use of stolen passports to enter the United States to ICE for investigation.

We recommended that ICE:

1. Develop procedures to investigate, locate, and remove from the United States persons that have used stolen passports to gain entry to the country and to report the outcomes of its investigations to CBP; and,
2. Investigate the activities while in the United States of the aliens that used certain stolen passports and determine their current whereabouts.

CBP and ICE concurred with all of our recommendations and plan appropriate corrective actions. While our office believes that these actions have been undertaken, we have not performed any formal compliance review.

One concern noted in our report is international in scope, and will require an international solution, i.e., the ill-defined process by which each country's stolen and lost passport information is reported and disseminated among all the other countries. The department's information about stolen passports is often incomplete. It's our understanding that INTERPOL plans to expand and regularize the reporting of lost and stolen passports. This initiative, when fully implemented with all nations participating, should permit automatic checking at the port of entry to determine whether the traveler is presenting a lost or stolen passport.

Even with the completion of the corrective action we recommended, the VWP will always pose some security risk. The fundamental premise of the program is that millions of persons, about whom we know little, can be exempted from DOS' ever more rigorous visa procedures and permitted to board U.S.-bound planes. As we said in our report, "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 visa interview DOS has collected and stored considerable information about the traveler and the traveler's planned journey. DOS has introduced biometric features into its visas, shares data from its visa records with DHS port of entry systems, and significantly increased the percentage of applicants subject to a careful interview. In contrast, the visa waiver traveler is interviewed briefly, and the passport examined, again briefly by an inspector who may be unfamiliar with even valid passports from the issuing country.

One of the most significant corrective actions responsive to the concerns stated in our report is the processing of visa waiver travelers through U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). As implemented in December 2003, US-VISIT excluded visa waiver travelers from its scope. We strongly recommended that visa waiver travelers be added to the US-VISIT program because of the additional screening, identification, and exit control features it offers. On April 21, 2004, DHS Secretary Ridge announced that BTS would begin to process visa waiver travelers through US-VISIT by September 30, 2004.

This brings me to another pressing border security matter much in the news recently—our land borders.

US-VISIT at the Borders

In February 2005 we released our inspection report on the implementation of US-VISIT at land border ports of entry.[3] The report was written because legislation mandated the implementation of an automated, integrated entry exit system at the 50 highest volume land ports of entry by December 31, 2004. We reviewed efforts undertaken by the US-VISIT Program Office to meet this deadline, develop imple-

[3] "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports of Entry" (OIG–05–11) February 2005.

mentation and deployment plans, modify existing facilities, conduct or plan pilot testing of systems and new technology, and achieve program goals.

The examination of entering travelers at land POEs presents special problems. For one, CBP officers do not have an opportunity to prescreen using aircraft and ship passenger manifests. At land POEs there is less use of automation to check watch lists and other databases as part of the screening process. Indeed, name checks are not run at all on the vast majority of entrants. At present, travelers entering the United States at a land Port of Entry are only processed through US-VISIT if they enter on the basis of a visa. This is a very small percentage of travelers. The US-VISIT enrollment at land ports of entry will include approximately 2.7 % of the foreign visitor population. Why is this percentage so small? There are several reasons.

Mexican Border Crossing Card (BCC) holders entering the United States are not likely to have their entry electronically captured, nor their identity verified. Most BCC cards are visually inspected by Customs and Border Protection (CBP) officers, not scanned at primary inspection. As a result, the BCC holder's identity is not verified nor the entry electronically recorded. BCC holders accounted for nearly 43.8% of foreign national land border crossings in FY 2002.

Visa exempt Canadians, who represent approximately 22% of foreign national land border crossings in FY 2002, are also exempt from US-VISIT enrollment. They are able to gain admission to the United States by providing documents with limited information to verify their identities. The procedure is similar to that for BCC entrants—visa-exempt Canadians are not likely to have their entry recorded, or their name checked against any watch list.

Lawful permanent residents (holders of green cards) represent 32% of all foreign entrants. It is not standard procedure at a land POE to screen their names or record their entries.

Together all of these categories of foreign entrants represent two-thirds of the total at the land POEs; the other third are American citizens. American names are not screened against watch lists, and their entries are not recorded. The problem for border security is the possibility that someone is posing as an American, who is not an American. Detection of such imposters is weakened by the absence of automated and biometric checks.

Thus, while US-VISIT offers potential, few travelers are actually covered. Moreover, while US-VISIT may have met minimum statutory requirements for implementation at land borders, it lacks the exit component necessary to identify those who overstay the terms of their admission.

In addition, when trying to establish an individual's identity and determine admissibility, CBP officers currently perform queries of multiple information technology systems, many of which employ old technology and cannot interface. Achieving system integration becomes particularly important at land ports because inspection time is limited and there is no advance passenger information.

Fully implementing a comprehensive solution of integrated systems, processes, and data for electronically tracking the pre-entry, entry, status management, and exit of all classes of foreign national visitors seeking admission to the United States will be a complex, technologically challenging, and expensive project that will not be realized for at least five to ten years.

Current Initiatives

The recently enacted Intelligence Reform and Terrorism Prevention Act of 2004 requires that, by January 1, 2008, all travelers must provide evidence to establish identity and citizenship when entering the United States. Specifically, it requires that DHS develop and implement, as expeditiously as possible, a plan that requires a passport or other document, or combination of documents that sufficiently denotes the identity and citizenship for all travelers entering the United States. This includes not only those categories of individuals for whom documentation requirements had been waived previously but also U.S. citizens.

This represents a bold step towards exercising better control of our borders. As the GAO clearly documented in its unclassified testimony GAO–03–713T "Counterfeit Documents Used to Enter the United States From Certain Western Hemisphere Countries Not Detected", and its Limited Official Use report GAO–03–782 "Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process", our land borders are easily breached by imposters with phony birth certificates and driver's licenses.

The dialogue over how to improve document integrity, to track arrivals and departures, to employ biometric identifiers, which biometric identifiers to rely on, and how to automate screening transactions will continue. So will our office's monitoring of these very important programs.

Mr. Chairman, this concludes my remarks. I will be pleased to answer any questions the Subcommittee may have.

Mr. HOSTETTLER. Thank you, Mr. Skinner.

Mr. Shaw.

TESTIMONY OF JOEL F. SHAW, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BIODENTITY SYSTEMS CORPORATION

Mr. SHAW. Thank you, Mr. Chairman.

As you indicated in your opening remarks, I am the Convenor of the International Standards Organization (ISO) Working Group that is working with the International Civil Aviation Organization. As Convenor, I'm coordinating ISO's contributions to the realization of the new biometric passport.

Introducing a new passport, especially one integrating such a significant number of new technologies, while conforming to a new global standard and guaranteeing successful operation throughout the life of that passport is a very complex undertaking indeed. The level of complexity increases significantly in this case because a computer chip is being introduced into a traditional passport book, and that is being done to ensure that the data that is being carried for biometric identification is globally interoperable across the entire world. Our goal in doing this is to improve facilitation while strengthening security for international travel and border clearance.

Governments involved in introducing the new biometric passport have been required to contribute to the creation of an extensive array and set of international specifications and standards. They have had to introduce enabling legislation to deal with the capture and processing and holding and sharing of biometric data on their citizens. They have had to become proficient in a range of new technologies which have been deemed until this effort began as completely foreign to passport fabrication. They have had to integrate a computer chip into the passport book and introduce new machines supporting assembly. They have had to introduce the entire technological and process components to support the biometric capture. And they have had to do the very same thing to ensure that the standardized security schema is in place to protect the data that is on that chip. And they have had to as well introduce new processes and technologies across their entire issuance process supporting passports.

In addition, those people that are doing inspections have had to introduce processes and technology to realize a new process of inspection, one offering both improved facilitation and enhanced security.

Any nation that would undertake such renewal of its passport and issuance operation would do so over many years. Visa waiver nations have been asked to undertake all of this work adopting a very challenging time line.

I cannot comment on all of the visa waiver nations, but those that I am familiar with have chosen to deliver a new passport that works and can be counted on to deliver the enhanced level of security demanded by a post-9/11 world. I think it's important to share with this Committee that the new international standard for bio-

metric passport provides for deployment of a series of escalating security measures.

First, it contributes a preemptive measure in the form of new checks that can be implemented by an issuing state to prevent persons from securing a passport fraudulently. This is a accomplished by using the globally standardized face biometric technology to confirm the person renewing the passport is the rightful holder of the previous issued passport and to carry out lookout and fraud checks on each and every passport applicant.

Second, it provides an immediate detection measure in the form of a face-based lookout check that can be implemented by a receiving state on all persons seeking entry into the state. This new type of lookout check is not dependent on the availability of the new biometric passport. It simply requires the receiving state to install the face biometric capture technology and activate a check for persons deemed to be of concern to the state.

Third, it provides an escalating measure in the form of a positive identity confirmation check that can be implemented by a receiving state when persons present a new biometric passport during border inspection. This measure increases in security value as more and more traditional passports are converted to the new biometric type.

Although not part of the biometric program per se, ICAO is contributing an important fourth measure: It is working with Interpol to create a mechanism whereby receiving states can be informed immediately of lost and stolen passport numbers. This will ensure that reuse of stolen traditional passports, including blank books, can be detected immediately.

The question this Committee is being asked to consider is whether to extend the date of the 26th of October 2005. Based on the knowledge of the issues being faced that I'm familiar with and the understanding of the significant benefits that will be realized both for facilitation and security, I encourage the Committee to recommend the following:

The date of 26 October 2005 remain unchanged, but if exceptions are needed they should be made on an individual case-by-case basis;

Visa waiver nations that need more time to introduce their biometric passport be required to specify what they still need to do to come into compliance and propose a timetable for completing those tasks, and that extensions, if necessary, be granted on merit;

The visa waiver privilege be continued while the country comes into compliance;

And a far more prescriptive requirement be applied governing immediate sharing of lost and stolen passport information using the new computerized system established by Interpol.

I would like to thank you for this opportunity to address the Committee, and I'm very pleased to answer any questions you might have. Thank you.

[The prepared statement of Mr. Shaw follows:]

PREPARED STATEMENT OF JOEL SHAW

Good afternoon. My name is Joel Shaw and I am the Chief Executive Officer of BioDentity Systems Corporation. I recognize the importance of the issue being considered by this Committee and the impact the outcome will have, not only for those countries designated as US Visa Waiver Program nations, but equally, those coun-

tries that are moving to strength their own travel document issuance process and border controls.

I can offer this Committee a unique perspective; for in addition to being the CEO of BioDentity I am also the Convenor of the Working Group set up by the International Standards Organization (ISO) [headquartered in Geneva] to work with the UN's International Civil Aviation Organization to create international specifications and standards for official travel documents such as passports, visas and Official Documents of Identity. As Working Group Convenor I am coordinating ISO's contributions towards the realization of the new biometric passport. I am equally an experienced practitioner, having assisted the US Customs Service create and deploy the first passport readers used for border inspection, as well as help INS create and deploy their first computerized entry inspection system.

Introducing a new passport, especially one integrating such a significant number of new technologies, while conforming to a new global standard and guaranteeing successful operation throughout the life of the passport is a complex undertaking indeed. The level of complexity increases significantly in this case because a computer chip is being introduced into a traditional passport book, one that will hold biometric details enabling deployment of machine-assisted identity confirmation designed to improve facilitation while strengthening security for international travel and border clearance.

Governments involved in introducing the new biometric passport have been required to:

- Contribute to the creation of an extensive set of specifications that will ensure that the new passport can be read no matter where it is presented in the world;
- Introduce enabling legislation to support the capture, use, retention and sharing of biometric data on their citizens;
- Become proficient in a range of new technologies, which had been deemed, until this effort began, as completely foreign to passport fabrication;
- Integrate a computer chip into a passport book and introduce new machines supporting assembly, while at the same time ensuring long term durability and of course, successful operation;
- Introduce face biometric capture, create and deploy quality assurance standards and introduce new technology designed to ensure the highest quality biometric sample is recorded in the passport;
- Introduce the necessary processes and tools to address the standardized security schema to protect the data recorded in the computer chip;
- Introduce the necessary processes and technology to establish a new issuance process;

And for those wishing to inspect persons presenting these new passports,

- Introduce the necessary processes and technology to realize a new process of inspection: one offering both improved facilitation and enhanced security.

Any nation that would undertake such renewal of its passport and issuance operation would do so over many years. Visa Waiver Program nations have been asked to undertake all of this work adopting a very challenging time line!

I can not comment on all Visa Waiver nations, but those that I am familiar with have chosen to deliver a new passport that works and can be counted on to deliver the enhanced level of security demanded by a post 9/11 world. The new international standard for biometric passports provides for deployment of a series of escalating security measures.

First, it contributes a pre-emptive measure in the form of new checks that can implemented by an Issuing State to prevent persons from securing a passport, or any form of travel document, fraudulently. This is accomplished by using the globally standardized face biometric technology to confirm the person renewing a passport as the rightful holder of the previously issued passport, and to carry out Lookout and Fraud Checks on each passport applicant.

Second, it provides an immediate detection measure in the form of a face based Lookout Check that can be implemented by a Receiving State on all persons seeking entry into the State. This new type of Lookout Check is not dependent upon the availability of the new biometric passport, it simply requires the Receiving State to install the face biometric capture technology and activate a check for persons deemed to be of concern to the State.

Third, it provides an escalating measure in the form of a positive identity confirmation check that can be implemented by a Receiving State when persons present

a new biometric passport during border inspection. This measure increases in security value as more and more traditional passports are converted to the new biometric type.

Although not part of the biometric program, per se, ICAO has contributed an important *fourth measure*—it is working with INTERPOL to create a mechanism whereby Receiving States could be informed immediately of lost and stolen passport numbers. This will ensure that reuse of stolen traditional passports, including blank books, can be immediately detected.

The question this Committee is being asked to consider is whether to extend the date of 26 October 2005, and in so doing grant an extension to those Visa Waiver Program nations that are still dealing with their deployment challenges.

Based on an extensive knowledge of the issues being faced and an understanding of the significant benefits that will be realized both for facilitation and security when this program is successfully completed, I encourage the Committee to recommend:

- The date of 26 October 2005 remain unchanged, but if exceptions are needed they should be made on an individual case by case basis;
- Visa Waiver Program nations that need more time to introduce their biometric passport be required to specify what they still need to do to come into compliance and propose a time table for completing those tasks, with extensions to the date being granted based on merit;
- The Visa Waiver privilege be continued while the country with the exception comes into compliance; and
- A more prescriptive requirement be applied governing immediate sharing of lost and stolen passport information using the new computerized system being established by INTERPOL.

I would like to thank you for the opportunity to address the Committee. Mr. Chairman, I would be pleased to answer any questions the committee might have.

Mr. HOSTETTLER. Thank you, Mr. Shaw.

At this time we will turn to questions from Members of the Subcommittee. First of all, Ms. Dezenski, in your oral testimony, I believe you stated this, but just to clarify. The Department of Homeland Security has incorporated many of, if not all, the recommendations of the IG's report. Does one of those include a formal process of informing ICE when a fraudulent passport has been used at a port of entry but the individual has made their way into the country because we did not have notification that their passport was lost or stolen until after the point?

Ms. DEZENSKI. Yes, each of the recommendations that we received from the IG have been addressed, including that one, so there are formal processes now for those referrals. We've strengthened both in terms of what do we do if we get a lookout hit and we have to deal with that person at secondary, and what do we do if that information on lost and stolen passports comes after the fact and we do a check and realize that that document may have been used.

Mr. HOSTETTLER. Do you know how many times you've had to do that, how many times you've had to inform ICE of that?

Ms. DEZENSKI. That's a great question. I don't have that number, but we can follow up and get back to you.

Mr. HOSTETTLER. If you would please, for the record.

Mr. Skinner, how many stolen passports have been found in the hands of terrorists or potential terrorists trying to enter the country? For example, did not three British nationals just recently indicted for trying to blow up financial institutions in the U.S. enter on the Visa Waiver Program?

Mr. SKINNER. Our work that we have performed, hasn't identified that type of information, but, yes, you are correct. The three

British nationals that were arrested recently did, in fact, have passports. But let's keep in mind these were not stolen passports. These were legitimate passports. In fact, some came through on, I believe, student passports, but we have not validated that. But they were, in fact, legitimate passports. These were nationals and citizens of the U.K.

Mr. HOSTETTLER. Okay. Have al Qaeda terrorists anywhere in the world been found with stolen passports from visa waiver countries?

Mr. SKINNER. Well, to say they're terrorists, I don't want to go so far as to say they're terrorists because we don't have that type of evidence. But there is—there are coincidences. For example, there was the assassination in Afghanistan a couple years ago, and those individuals were apprehended. They had passports that were stolen from a batch of 46 passports.

We learned that, from that same batch of 46 passports, five—or at least six of those passports were used to attempt to enter the United States. Five of them were used successfully; one was, in fact, caught. But there are five individuals that were able to get through our U.S. ports of entry with stolen passports. They came from the same batch that was used by al Qaeda or individuals that were associated with al Qaeda in the assassination in Afghanistan.

Mr. HOSTETTLER. Is there any reason to believe that they still may be in the country?

Mr. SKINNER. I don't have any—you'll have to ask—I believe ICE might be able to give you the status of where those individuals are. But at the time of our review, yes, they were still in the country, or there's no evidence that they had exited the country.

Mr. HOSTETTLER. Thank you.

Mr. Veestraeten, when did Belgium—if I could get a timeline, when did Belgium begin your program to produce tamper-proof passports with biometric identifiers? And how long did it take you to put—to roll those first sets of passports out?

Mr. VEESTRAETEN. Mr. Chairman, after the PATRIOT Act was adopted in the U.S., we became conscious of the fact that we would have to move quickly to tackle this issue. I believe that I was here in Washington, D.C., in November 2003 for a first round of consultations with the American authorities—State Department, DHS—and so I think that we then made this—we engaged ourselves to be ready by—in the time frame of 1 year. We have aimed for October 26, 2004, which was the original deadline in the bill, and I think we were actually ready. We delayed a little bit. We started November 15, 2004, with the first deployment, and we had the full rollouts January 30. That was basically because of internal Belgium reasons. Because we still had a stock of non-electronic passports, we wanted to use the very last one of those in order not to waste taxpayers' money. So we were effectively ready by October 26, 2004, for the rollout of these ePassports. It took us about a year, I would say.

Mr. HOSTETTLER. Very good. Thank you very much.

The Chair now recognizes the Ranking Member from Texas for 5 minutes.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. I also want to acknowledge my colleagues who have joined us, Congress-

man Berman and Congresswoman Waters, who are here part of the hearing.

I'd like to, before I start, Mr. Chairman, ask unanimous consent to have submitted into the record the TIA letter, Travel Business Roundtable, dated April 21, 2005.

Mr. HOSTETTLER. Without objection.

Ms. JACKSON LEE. Thank you.

Ms. JACKSON LEE. Mr. Chairman, this is an important hearing, and I think we have the opportunity for additional hearings. I'd like to ask the Chairman his—or request that we have an opportunity to hear from the State Department and ask the Chairman whether or not he asked the State Department to participate in this hearing, whether or not we'll have a second hearing, whether or not the State Department will be present.

Mr. HOSTETTLER. It's very possible that we could have another hearing on this issue. We have a limited number of seats, according to Committee rules, and we felt that this was an excellent mix. But the State Department would obviously have excellent input and insight on this very important issue. It's possible that we may have a hearing in the future.

Ms. JACKSON LEE. Mr. Chairman, then let me orally make a formal request for the State Department's participation, and I will be instructed by your staff how to make that in writing or a more formal request. But let me for the record ask that we do have an additional hearing that will allow for opportunities for possibly other visa waiver representative—meaning countries, their representatives be present and/or the State Department—not and/or but and the State Department. I think that would be a crucial part to part of the work that we're trying to do, particularly in asking them direct questions about the issue of their protection of stolen passports.

Mr. HOSTETTLER. We will take that under consultation.

Ms. JACKSON LEE. I thank the Chairman. I hope in the course of the dialogue with staff it hasn't gone from consultation to a good possibility of a hearing, but I thank you very much and I will be engaged with you on that item.

Let me—Mr. Veestraeten, if I'm getting it almost right, welcome. I wanted to just to your point, if you can explain or elaborate. You said let's look to inclusiveness and not exclusiveness. Why don't you expand on that for me, please?

Mr. VEESTRAETEN. Well, what I want to say is that we are all in the same struggle to bring the technology into the passports, that is, the whole of the European Union, not only Belgium, that is, including the U.S., Canada, Australia, New Zealand. All those countries are working hard on electronic passports and on the compatibility with ICAO standards.

Some countries have had more difficulties than others for different reasons. Historic background may be one also. There are also different mechanisms in different countries for changing the way a passport is produced. Some countries were already in a completely centralized system like we were lucky to be there. So it was easier for us to implement new technology than other countries which do not yet have a completely centralized system for passport issuance.

All these things are important. What I want to say is that we all are there together. The Visa Waiver Program is for Europe of the utmost importance. It is a reciprocal facility to travel for Americans and for the Europeans. I would very much regret that while we are all doing our best to get where we want altogether to be, that at such a moment the program itself might be in danger. That is what I mean with those words.

Ms. JACKSON LEE. You want us to be able to find as reasonable a solution as possible, keeping in mind the needs of security. And I might add for the record that both Spain and Italy, which were also allies in the Iraq war, are included in the possible denial of the extension.

Let me ask Ms. Dezenski about the issue dealing with your—the lookout system and if Mr. Skinner would comment after you comment. You believe you've made some progress, and let me applaud you. I believe there have been some steps. But there are criticisms. How committed are you or how convinced is DHS that they are working through the problems of the lookout system and they've really met the standards, the test that the IG has offered in his report?

Ms. DEZENSKI. We do think that there has been marked improvement in terms of the type of information that we're getting, particularly through the Interpol process, and then being able to implement that into our systems and get that out to our border inspectors in a quicker fashion, and it's more comprehensive information. So I think we feel cautiously optimistic that this is moving in the right direction.

Now, we will be monitoring this very closely. We've stood up a new organization within DHS called the Office of International Enforcement, and their primary goal is to monitor the VWP program and ensure that the criteria are being met. And, in fact, I mentioned in my oral statement that we're just completing our review of the countries, and that happens on a 2-year basis. So once we complete this, we'll be just about ready to start the next review.

So it's an iterative process of ensuring that these foreign partners are living up to the standards, and with specific respect to the lookout system, we think that the types of information we're getting are better and we're making progress.

Ms. JACKSON LEE. Mr. Skinner?

Mr. SKINNER. Yes, I must agree. The Department is, in fact, making progress and it is getting better on a monthly basis. It does take time, but other elements within the Government are now contributing more. We're getting more concise data. The issue with the Interpol is probably one of the things that we're most pleased about, to get those countries participating.

I would like to point out, however, it's not necessarily always the lookout system that's at fault here, because they are getting information and they are developing a huge inventory.

One of the underlying problems here is the two numbers that we use on our passports and that this country as well as other countries use. And this is particularly important when you're dealing with stolen blank passports, because what is reported is the blank—or is the passport inventory control number, not necessarily the passport number. So once that document is forged and used to

come into this country, our capability to identify or to match the passport number with the inventory control number currently doesn't exist. And therein lies the problem, and until we start using one number on our passports for the inventory control number as well as the passport number, we're going to continue to have problems and people are going to still continue to get these passports or use these passports to get into this country illegally.

Mr. HOSTETTLER. I thank the gentlelady.

The Chair now recognizes the gentleman from California, Mr. Lungren, for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate this, and I appreciate the fact that you have set up this meeting. This is an extremely important issue.

Mr. Shaw, you indicated in your written testimony and in your oral testimony that this is a complicated process, that is, what we are asking to be done with respect to these enhanced passports. I understand that. I also remember the Manhattan Project may not have taken as long as many of the things we're asking us to do in these days.

I came back here because of 9/11. I came back after being gone 16 years because it seems to me the world had changed and we needed to act as if the world has changed. And one of the big disappointments I have is not everybody seems to act that way.

How long is reasonable? I mean, in your written testimony you said the date of 26 October 2005 should remain unchanged, but exceptions, if needed, should be made on an individual case-by-case basis. So, it sounds like you expect that there are exceptions, there should be exceptions. How long should we expect to wait? And is it because in your estimation, not the complexity because you say keep the date there, but the lack of political will or practical will? Or what is it we're facing here?

Mr. SHAW. Well, I cannot speak on the political will for the various countries, but I can speak on the technical complications.

I would say, first of all, that within a year after that date you should expect all of these countries to be in complete compliance. No longer than that.

Mr. LUNGREN. So that the outside date would be 26 October 2006, as far as you're concerned, for any and all——

Mr. SHAW. Of the countries, absolutely. I think the issue is that each one is facing a different situation, and what we're really asking the various countries to do is to get in lockstep. This data that is being put on the passports, which is the biometric data, has to be able to be used and interpreted all over the world. And I think this is where the complexity lies because the books are all different. There's an individual way that these countries make passports. You're trying to integrate the chip into the book and at the same time to introduce biometric capture and have a mass public participation and a machine-assisted confirmation scheme and have no mistakes in it. When they arrive in this country, they're to work.

Mr. LUNGREN. I appreciate that, and I understand the complexity and the difficulties of all sorts of countries marching in lockstep. General Eisenhower had to confront that on D-Day. Thank God he

didn't have extension—in fact, he didn't extend the time beyond one day, as I recall.

If I could ask the representative from Belgium, the Director General from Belgium, you folks seem to have been able to complete this mission. Can you tell me from the standpoint of your government, what were the most difficult challenges? Were there legal challenges, practical challenges, or political challenges in making sure that you were able to accomplish this task?

Mr. VEESTRAETEN. I think for us it was practical. Most difficult was the practical challenge. Political challenge, we knew we were—the government was very much convinced of the fact that we needed to be in compliance. I think the problem was mostly practical.

I just wanted to point out for your information two elements. First is that indeed we do have only one passport number. I didn't know the countries had two different passport numbers in their passports. This seems to be indeed the reason for confusion. So since a long time, we only have one single.

The second thing is that there is a deadline, not a U.S. but the European deadline, for passports with a computer chip, and that deadline has been set by the European Commission and the member states. It is August 28, 2006. So by the end of August 2006, there is an internal European regulation which puts a final deadline for all member states, all 25, not only the Visa Waiver Programs, to include a computer chip in all individual passports issued after that date.

Mr. LUNGREN. Thank you very much.

Ms. Dezenski, if, in fact, we get everybody to cooperate, at whatever date we do, is the Department of Homeland Security prepared to actually utilize this? That is, do we have the equipment purchased? Do we have the efforts in place so that we can actually read these things and make sure that they are functioning so that we don't on our end have a delay?

Ms. DEZENSKI. One of the most challenging pieces of this has been the reader technology and ensuring that we procure the right readers to read the right types of identifiers. We have a pretty robust process over the next 3 months to continue testing in live operational environments several different types of reader technologies so we can make a procurement decision that reflects some data, that will give us a better sense for what will survive in a very busy environment. So we are moving forward with that and certainly are committed to getting those readers out——

Mr. LUNGREN. What is the date certain?

Ms. DEZENSKI. —as soon as we can. I can't give you a date certain.

Mr. LUNGREN. I know. You told me the process is robust. You told me as soon as possible. You told me you're doing all those things—I love all that. But if I were in a courtroom, and I asked you that question under oath, the judge would probably tell you these were insufficient answers.

Ms. DEZENSKI. I can tell you that we will not have all readers deployed by October 26, 2005.

Mr. LUNGREN. Will not.

Ms. DEZENSKI. We will not make that deadline.

Mr. HOSTETTLER. I thank the gentleman.

The Chair recognizes the gentleman from California for 5 minutes, Mr. Berman.

Mr. BERMAN. Well, thank you very much, Mr. Chairman, and I congratulate you on having this hearing. My colleague from California, Mr. Lungren, made reference to General Eisenhower in meeting a deadline. Of course, U.S. troops were part of group that had to meet that deadline. He wasn't just telling the allies to meet that deadline. So my question is: Does the State Department now issue passports that meet the standards we are requiring as of next October, that is, a digital photo for facial recognition, plus optional biometrics of fingers and/or eyes which are stored on contactless integrated circuit chips? Do we now issue those passports to our citizens?

Ms. DEZENSKI. Obviously, the Department of State is not here to answer that for themselves——

Mr. BERMAN. But I'll bet you know.

Ms. DEZENSKI. I do know and, sir, no, they do not yet issue those.

Mr. BERMAN. Okay, so——

Ms. DEZENSKI. They are in the process of deploying a new passport which will go out for the first test phase, if you will, this summer. It will only be issued to Government employees. And then depending on how that process goes, they'll continue with deploying the new document to the broader public after that initial phase.

Mr. BERMAN. So if the Europeans imposed the standard on us and the other visa waiver countries imposed the standard that we're imposing on them, the U.S. would not be in compliance. American citizens would have to obtain visas at European consulates around this country in order to go to those countries.

Ms. DEZENSKI. We would not meet a requirement that would include a biometric chip within the passport document.

Mr. BERMAN. But that is our requirement for them, isn't it?

Ms. DEZENSKI. Correct.

Mr. BERMAN. Okay. Assuming the deadline passes, I mean, from what you've said, Belgium is ahead of the United States on this issue. Am I right?

Ms. DEZENSKI. I think the comments from the gentleman to my right would indicate that Belgium is leading the pack amongst VWP countries in terms of those biometric requirements, yes.

Mr. BERMAN. But for the countries that don't meet it, what will the State Department be faced with following the October deadline in terms of applications, manpower needs, things like this?

Ms. DEZENSKI. Sure, I think there's probably a couple of things to consider, and the first would be if the deadline continues as is, it would require a significant number of people to obtain visas before they come into the country. Right now we have about 40,000 people who come into the U.S. every day under the VWP program. So for those who are not in compliance with the requirement, they would be needing to go to the consular offices and obtain that visa to enter the country. So there's that issue.

There also issues in terms of workload associated with that that the Department of State would probably be better suited to answer and I know they've thought about some of those implications. But obviously there's a lot of back-end work to be able to accommodate that additional group of people.

And the other thing to consider from a travel and from a tourism perspective, the more layers that we have from a security perspective, we have to be even more cognizant of whether people will simply talk with their feet and decide not to travel to Disney World, not to travel to locations, because there are now one or two extra steps to go through to get the family here.

So those are the types of implications that we would need to keep in mind.

Mr. BERMAN. The Japanese Embassy has said that approximately 670,000 Japanese citizens will have to apply for visas based on current travel, 670,000 between October 26 of 2005 and March 2006. That will be, that particular country, quite a workload on our embassy and consulates there.

My final question then is: You're here on behalf of the Administration. Has the Administration—you've indicated the U.S. won't have such a passport ready by October 26. It's clear a number of other visa waiver countries won't. Has the Administration taken a position on the October 26 deadline?

Ms. DEZENSKI. Well, I don't have a mandate today to tell you about any shift in policy from what we've been pursuing thus far. Secretary Chertoff intends to be up here in early May to speak with Chairman Sensenbrenner about some additional——

Mr. BERMAN. About why he needs an extension.

Ms. DEZENSKI. About some additional details on what we think the recommended path forward might be.

Mr. BERMAN. Thank you.

Mr. HOSTETTLER. I thank the gentleman.

The Chair now recognizes the gentleman from Arizona for 5 minutes.

Mr. FLAKE. I thank the Chairman for calling this very important hearing. When we extended for a year last time, I stated at the time that it ought to be 2 years which the Administration asked for. Now we're seeing why that needed to be the case. And if nobody else is prepared to, I'm prepared to introduce legislation to go for another year, or two if we need to.

I met with the travel industry yesterday, and our economy is really taking it here because of this and many other things. It's the certainty going ahead. Our friends from Europe and other visa waiver countries simply don't have certainty going forward, so they don't plan convention visits or anything else. And it has to do with procurement of U.S. goods and everything else because they can't travel here or feel they may not be able to. And it's really hurting us, and I don't know what we're gaining by not extending it again or indicating that we are. So I hope that we move quickly to give countries more certainty, and I applaud the Belgians for moving ahead more quickly than anybody else. But when they're ahead of us, I can't imagine that we could expect the others to move any faster than that.

So, anyway, I just want to indicate my willingness to push ahead with another extension. I think that is what needs to be on the table, and then let's decide how long that extension needs to be. But we can't expect others to do what we're unprepared to do ourselves, and that's the bottom line.

I thank the Chairman.

Mr. HOSTETTLER. The Chair now recognizes the gentlelady from California, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman and Members. I'm just really remembering the last hearing that we had on this issue and some of the concerns that I had at that time.

First, let me just say that I understand that the technology for the development of the biometrics that's needed is not really complete, it's not reliable at this time. Is that correct?

Mr. HOSTETTLER. If the gentlelady will yield, this is an excellent——

Mr. SHAW. I yield to the——

Mr. HOSTETTLER. —opportunity to clarify that the standard that is being required by October 26 of this year is the standard, once again, that was in place in 2002, which was the biometric facial standard. This technology is in place. It's capable. The technology that you might be considering is the chip technology that is still——

Ms. WATERS. Yes, I'm talking about the chip.

Mr. HOSTETTLER. Right, but it is not required in current law. The country of Belgium spent about a year and was able to meet the requirements under law, the previous requirements under law. And so the technology that is required by law for the deadline is in place and can be used. So there's not a question of technology—and let's clarify that. There's not a question about technology or the standards that are required to meet the October 26, 2005, deadline. And I yield back.

Ms. WATERS. All right. Well, I mean, I think this hearing is very important, but I suspect that we are not prepared to disrupt the tourism and the trade and everything else that goes along with, you know, people being able to come to this country. So I'm not really focused on that so much. I'm glad that we're talking about it. I think that probably the extension is going to happen. I don't see any signs that anybody's willing to hold that up.

What I asked before is about the countries that participate in the Visa Waiver Program. Where is Andorra? What is it? Where is it? Anybody know? I know about these little places like Monaco and Brunei. But I see a number of countries on here that I don't know very much about.

I'm concerned about countries like South Africa. We have a major trade agreement, the African Growth and Opportunity Act, with South Africa. And, of course, there are no countries of color much in this list, but I'm concerned about what we can do to open up opportunities with the expansion, with the extension that we're going to give. I'm concerned about opening up opportunities to countries that are not listed. I know Andorra and Monaco may be very, very important, but places like South Africa I think are very important, too.

What can we do as we give the extension, what can do to open this up?

Ms. JACKSON LEE. Would the gentlelady just yield for a moment?

Ms. WATERS. Sure. I yield to the gentlelady from Texas.

Ms. JACKSON LEE. We have—I think what you have just opened up is the question of an overall review. Through the years of my service on this Committee, I've raised that very question on South

Africa and a number of other countries that are again being our trade partners but also our allies in war and peace. So I yield back to you by saying that this is why I believe this is an important hearing, but I think also we will need to assess what we're doing here today because we're either going to break the system by burdening offices around the world who cannot face the large numbers of visa requests, and then, of course, we've never addressed the question of whether or not that list can be expanded or diversified. You raise a very good question. I think we need ongoing hearings on this subject.

I yield back.

Ms. WATERS. Thank you very much. I appreciate that. And, of course, I would be willing to join with my colleagues for an extension, as the President of the United States and everybody else is going to do, but I would not be willing to do it without taking a look at how we expand this list, particularly to countries that we have trade agreements with, such as South Africa, where it's important for them to have this opportunity also.

So I yield back the balance of my time.

Mr. HOSTETTLER. I thank the gentlelady.

The Chair now recognizes the gentleman from Texas, Mr. Gohmert, for 5 minutes.

Mr. GOHMERT. Thank you, Chairman. I appreciate this opportunity. I appreciate you all coming forward to testify. Having been a judge for so many years, I'm familiar with what it takes to come forward and testify. I've done it myself.

But, Ms. Dezenski, Mr. Skinner, did you all ever see the original "Jaws" movie? You know what I'm talking about?

Mr. SKINNER. Yes, I do.

Ms. DEZENSKI. I've seen it.

Mr. SKINNER. I did.

Mr. GOHMERT. And do you remember how the police chief was really concerned about the public safety and that they had a real menace out there waiting to kill people, and the city council and the mayor, they just wanted to protect the tourism. And they got so concerned about the tourism that they quit worrying about public safety, and as a result, people got killed.

Now, it's my belief and my feeling from people in the district in Texas—and we have a huge number of folks, though I'm a Republican, that often vote Democrat for other positions—but I feel a huge sense of concern about this Government doing one of its principal functions, and that is, providing for the common defense.

If there is another attack and it turns out that once again we have been derelict in who had visas, who wasn't collected and gotten rid of, gotten out of the country, then I think there will be a wholesale change in Congress. If I am allowed to come back if that were to happen, I'm going to be looking to help there be a wholesale change in those that did not have a sense of urgency about the safety of this country. That includes with contractors, that includes with people within the Government, because I think we should have a sense of urgency. And that's where I'm coming from.

So with that understanding, I'm curious, and you may have answered and I haven't heard. I came late from the floor. But how

many VWP countries do you think will be able to meet the October 2005 deadline?

Ms. DEZENSKI. I'm consulting my cheat sheet here. We think that there are about 14 countries who are on track to be close to the deadline. One thing to keep in mind—this was touched on a little bit earlier. Based on that list of those countries, that's about 21 percent of the folks coming in under the VWP program. So the biggies, if you will—France, the U.K., et cetera—are further down in the list. So about 80 percent of the volume coming in under the VWP program would not be in compliance by that date.

Mr. GOHMERT. Okay. What's your assessment of how diligent those who will be in non-compliance have been?

Ms. DEZENSKI. I think there's been a tremendous good-faith effort. We've been working closely with these countries over the last—specifically over the last 2½ years on some of the things we're talking about today but more broadly over 6 years on improving the security of passport documentation. And I don't think that there's any lack of good faith, as I said, to meet these requirements. I think that it's technical and operational in nature, and we need to make sure that as we move forward we're deploying the right type of technology. We do not want to be in a position to procure readers, for example, that don't get us to the system that we need, both to facilitate people moving through the border inspection process and to ensure that, you know, we're able to read the documentation that we're now requiring.

So these are tough issues, and I don't think anybody wants to be in the position of not meeting a deadline, including our foreign partners. So I think there has, again, been a very concerted effort to move forward as quickly as we can.

Mr. GOHMERT. Let me ask Mr. Veestraeten, what kinds of problems have you had, if any, with your readers? Since you are out front, usually that's where problems make themselves known.

Mr. VEESTRAETEN. I don't think that we have had problems with the readers at the moment. They seem to work fine. We have deployed the readers at the national airports, and we have asked the police, the Belgian Federal police, to give us weekly reports on the results of those readings of chips. We're starting to get the first reports now, I think two, three weeks ago, and so far the passports which have been checked were fine.

Mr. GOHMERT. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. HOSTETTLER. I thank the gentleman.

The Chair now recognizes the gentleman from Iowa for 5 minutes.

Mr. KING. Thank you, Mr. Chairman, and I want to thank the panelists as well. I came in here at the tail end of this testimony, and so I'm kind of picking this up on the run. And I want to also reiterate the metaphor that Mr. Gohmert used. I'm sitting here trying to think of one, and he brought one up. But it does occur to me that there's a reason why we are doing this, and we had lost track in this discussion as to why we have established the Visa Waiver Program and set up this structure.

As I sit here and listen to the answers to the questions and what little I know about this history of this event—and it's probably not

all that minor—I have to ask myself this question. There's an advocacy here for an extension for the sake of the tourism industry, and particularly 670,000 Japanese. That's a pretty significant number and reason to consider this, and I've heard that issue come up several times. We recognize that in the European Union there will be a number of countries that won't be able to comply.

I see this date of August 28, 2006, where it looks like all the EU will be in compliance. So I also want to ask my first question to Mr. Veestraeten in case he may know that, or whoever else on the panel. Is that a date that will be met, do you believe, by all 25 members of the EU?

Mr. VEESTRAETEN. Well, to be honest, I'm not sure. I cannot talk for each of the individual countries. What I can point out, if you'll allow me for these deadlines, that the U.S. deadline is a deadline of another nature than, for instance, the previous one on the machine-readable zone. The machine-readable zone deadline in the U.S. legislation was one which brought an obligation both to foreign countries and to the U.S. Government to have this—obligation to have this technique incorporated in the passports. This is not the case for the chip, as you very well know.

There is, of course—and I don't want to qualify—to make a difference of which is the better way to go. There's another way to go which we have now adopted in Europe, which is to set a deadline for ourselves, but we have not yet developed any deadline for third countries at this point.

So I think that the fact that this is an internal deadline, it is, first of all, also a way to go. I did want to point it out. But it's also, I think, another nature of obligation because I think that countries will be—will feel compelled to also respect this deadline. I think there is an extra motivational element there. So I think that, yes, first of all, the date is a bit farther away, so it gives a little more room, about 10 months. But, secondly, I think that the motivation is there also for the whole of Europe to really be there by that time.

Mr. KING. I thank you. And, Ms. Dezenski, then to complete this circle of questions in a way, and that is, are we looking for an extension for the countries that aren't going to be able to comply for the tourism industry in the United States or for the Department of Homeland Security?

Ms. DEZENSKI. As I stated earlier, my goal today is not to broach that subject. The Secretary is planning to meet with Chairman Sensenbrenner in the beginning of May to chart out a more detailed path.

Mr. KING. Then I would state to the panel that it appears to me that our sense of urgency has dissipated over the last 3 years, 3½ years, and again reiterate Mr. Gohmert's remarks with the necessity for this, the reason that we are—we have moved forward on this. And if we can move forward at a pace that's comfortable to all of us, that wouldn't be a pace that I would be comfortable with if that means that the security of this nation is put at risk.

Thank you, Mr. Chairman. I yield back.

Mr. HOSTETTLER. I thank the gentleman.

Because of some desire from some Members of the Subcommittee, we're going to go for a second round of questions. I don't know how many we'll have. I will give myself 5 minutes to begin that, and

I would like to for the record clarify that every individual in a Visa Waiver Program country that has a valid visa today, if their visa does not come out of deadline by October—if it does not expire by October 26, 2005, will be able to use that passport subsequent to October 26, 2005. The deadline is for new issuance of visas. So of the 700,000 or so Japanese, of which we have a tremendous concern today that have a passport today, their passports are going to be able to be used after October 26, once again, until such time as they expire after that time.

Mr. Skinner, I'd like to ask you questions as well with regard to the lost and stolen passport database. Except for times when countries report that there have been a significant number of passports stolen from Government agencies, Government facilities, we, in fact, depend on individuals in Visa Waiver Program countries to report their passports as being lost of stolen. Is that not correct?

Mr. SKINNER. Yes, that's true.

Mr. HOSTETTLER. So they could be lost or stolen for a long period of time before the individual would report it to their government and then their government could virtually immediately report it to us. But there could be a significant amount of time theoretically that would——

Mr. SKINNER. Yes.

Mr. HOSTETTLER. —transpire between that time.

Mr. SKINNER. Yes, that's true, if they report it at all. They may not even report it.

Mr. HOSTETTLER. Exactly. And do we also not know that from time to time there are instances of individuals selling their passport and they would not have a desire to report that.

Mr. SKINNER. That's possible, yes.

Mr. HOSTETTLER. If they sold their passport.

Mr. SKINNER. Sure, that would be possible. That's not something that we investigated or that we included in our assessment. But, sure, that's possible.

Mr. HOSTETTLER. So there is this universe of possibilities, of potential situations that are out there that your recommendations and DHS' subsequent implementation, there is a universe that will not be covered, potentially not be covered by these suggestions.

Mr. SKINNER. Yes, that's true. But we should point out that when you're dealing with a passport that has been issued, they are very, very difficult then to alter. And if they are altered to enter the United States, then I think our inspectors are very well trained to identify them. So they're a lot harder to use, unlike the blank passport, wherein those can be more easily altered. But when you're dealing with someone's picture that has to be altered, a lot of these passports that are used today are digital photos, that's almost virtually impossible to—without destroying the passport itself—to alter.

Mr. HOSTETTLER. Thank you.

Mr. SKINNER. So it makes it very difficult.

Mr. HOSTETTLER. Thank you.

Mr. Veestraeten, how does Belgium deal with the illegal sale of passports? Do you have a statute, do you have a law in place that deals with that?

Mr. VEESTRAETEN. Yes, of course, Mr. Chairman, we have laws against fraudulent documents, people who make them and so on. We prosecute people who we find trafficking documents or altering documents.

Mr. HOSTETTLER. Very good. Thank you.

The Chair now recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Thank you. We've heard a wide range of testimony today, and we've even had one of our artistic giants in the movie industry being utilized to explain the need for homeland security. I am trying to think of one equally popular and comes to mind "Beauty and the Beast," which was a popular movie as well. And I think when we talk about making choices, it should be a practical discussion. And, frankly, the Visa Waiver Program was a practical program that dealt with the comings and goings of countries that had longstanding relationships.

At the same time let me be very pointed. Democrats have been very strong on homeland security and remain so, and I think it is important to note—Mr. Skinner, you were in another hearing that I managed to come in because I was in Judiciary, but we spoke about the management issues. And I believe I raised—though you did not have an opportunity to speak to my question—the challenge of integrating 180,000 persons in the Department of Homeland Security. And so I understand Ms. Dezenski's step-by-step effort to respond to your concerns out of the IG, but we must be practical and realistic.

I guess let me just ask this one question to you. Does the Visa Waiver Program equate to you to equal terrorism?

Mr. SKINNER. No. I would not go so far as to say that. There are risks out there with the Visa Waiver Program. As I said earlier, the mere fact that you don't have to go through the rigors of a visa review process coupled with the laws of our partners in other countries, to be able to be naturalized, that presents a problem for people such as Reid who tried to bomb a plane with a shoe bomb. He was a naturalized citizen. The three individuals who were apprehended in England who had visited this country on multiple occasions, who had been associated with al Qaeda, I think two of those three were naturalized citizens. And I think those issues——

Ms. JACKSON LEE. Those are problems that we have.

Mr. SKINNER. Yes. These people, and those issues are the types of things that we need to be concerned about, and there's where we get into our intelligence operations. We have to have a very robust intelligence program to be able to be prepared to address those type of issues.

Ms. JACKSON LEE. I appreciate that distinction, that the program itself is not the problem. It is obviously a program we have to give great oversight, but we need other integrated functions, such as intelligence, to discern the difference between individuals coming for good and individuals coming to do harm.

Mr. Shaw, you gave solutions, and I thank you for being a witness today. Would you re-emphasize those solutions? In fact, I think the interest is—one main question that I have, if I can just share it with you, and if you can answer the question. What can go wrong if visa waiver countries are rushed to meet the deadline?

You offer some technological solutions, and if you can include that in your answer.

Mr. SHAW. Well, I think the biggest problem will be they'll all show up with a passport that won't work because, irrespective of what is happening, the new biometric passport has one incremental, additional component. It's allowing machine-assisted identity confirmation. You'll have chaos at Homeland Security because they'll show up, and it says I can't read the data from the chip, I can't identify the person, then immediately the person is suspect. Is it because they've done something to the chip, or what is it? And I think that this is what I'm seeing now in the work that I'm doing across the world, that countries are vigorously trying to make sure that that identity detail that goes onto that document works when they arrive in the United States.

Ms. JACKSON LEE. So what you're seeing across the world is that the countries in particular dealing with the visa waiver are making efforts, are working through the technology, are trying to get a refined process. Is that my understanding?

Mr. SHAW. Absolutely, and are vigorously testing and experimenting. One of the countries that's been mentioned—I won't be specific—that is going to be delayed actually has conducted a major test of not only facial but fingerprint technology recently. And so they're going to through an extensive array of testing to make sure that that one thing that is supposed to happen when they arrive in this country works and that is that they can confirm identity.

Ms. JACKSON LEE. And I guess the idea is that if we don't focus on allowing that technology to be improved, we may create a greater nightmare than what we would have.

Mr. SHAW. I would say so, yes.

Ms. JACKSON LEE. And that speaks to your suggestion that let them be in an ongoing process of compliance by making an ongoing assessment of their work toward being in compliance.

Mr. SHAW. Absolutely.

Ms. JACKSON LEE. And not shut the door completely on that.

If I can make this final point, Mr. Chairman, I was speaking with some individuals earlier today about some technology that might be used inside the United States, because people do come in and then travel around. The potential of being able to discover very quickly whether or not a Sheila Jackson Lee boarded a plane in Chicago and then all of a sudden showed up at the L.A. airport in not sufficient time to have gotten in both places, technology would immediately hold one of us. I think the key is you'd want the technology to work so that it's either holding the right person or there was not a confusion in the name. That's only a simple explanation of what I think I hear you saying and what these international entities are trying to do and that we do need to pay attention to what would happen stateside if they came with the wrong technology or the inappropriate document.

Mr. SHAW. Absolutely. I heard an official at one point in the international meetings we were in say that if the biometric doesn't work, we're going to send them to secondary. And the response was you're going to have a crowded secondary, because the technology is an empowerment tool for the border inspector. They can look at the image that's on that screen and confirm that the person stand-

ing before them is exactly who they say they are. That's why face was chosen, because it's a redundant capability. You've got to have this capability if the equipment fails, and that's what this is all about. So you want to make sure it does work.

Ms. JACKSON LEE. I thank the Chairman.

Mr. HOSTETTLER. Thank you.

The Chair now recognizes the gentleman from Texas for 5 minutes.

Mr. GOHMERT. I'm going to yield back the time to the Chairman.

Mr. HOSTETTLER. I thank the gentleman.

Mr. Shaw, if I can ask you one question, with regard to the use of technology for screening devices that will accept—essentially readers that will accept the passports, the presence of a chip will not preclude a level of technology or a generation of reader that simply recognizes facial biometrics. The presence of a chip, regardless of its status, whether it's maturer technology or not, will not preclude the use of a facial biometric identifier and reader to operate properly. Is that correct?

Mr. SHAW. No, it will not.

Mr. HOSTETTLER. Okay. So even for countries that—I said I was going to ask you one. Here's two. Even for countries that are looking for advanced technology such as the chip, if they simply meet the requirement of the facial biometric and the other requirements according to the 2002 act, those passports will still be usable in the United States given that we have the technology to read those passports, correct? Regardless of the presence of a chip or what type of chip or the maturity of the technology or anything like that.

Mr. SHAW. If I understand you correctly, the chip was chosen because we had to have the capacity, a large block of memory, to put data on in a way that was globally interoperable. There are many, many facial recognition algorithms, and if we put down the mathematical representation, let's call it, the template, then you'd have to buy proprietary technology and have a row of different reading devices to analyze that data.

So what happened was that we went to a globally interoperable representation, which is the facial image, and that increased the capacity. There was also the potential of incorporating fingerprint, potentially iris data, increase the size of the tank even more.

So one of the reasons a chip was chosen, because it's forward-looking, is it allows the capacity to be expanded, and allows someone to put on all three biometrics if they want, or just one. And that was one of the reasons why we went to the chip and it has been a cornerstone of the ICAO decision. And it's been done for one reason: global interoperability.

If the gentleman will continue to yield for just one more question. But the chip is not required for the fundamental reading of the facial biometric.

Mr. SHAW. If the data is put on the chip—or onto the passport, recorded on the passport, yes, the chip is required, because that's where the encoded data is, is in the chip.

Mr. HOSTETTLER. But it's—all right. I'll have questions I'll submit.

Mr. GOHMERT. No, go ahead.

Mr. HOSTETTLER. Well, but we do not require the chip by law. The chip is additional to the law and can be used for supplemental information and later generational technology information. But to actually read the facial biometric for a reader you don't need the chip to talk to the reader. You simply need the facial photograph, correct?

Mr. SHAW. The original convention had three basic potential ways of dealing with this.

First of all, you could take and scan the photograph that's in the data page of the passport. That requires a special reader. The chip is used to encode it in a way that gets around some of the problems of scanning through laminate and security features and things like that.

Mr. HOSTETTLER. Right.

Mr. SHAW. But the other aspect of it is that if you're not going to do a positive identification—in other words, identifying you as who you say you are, then the facial recognition technology can run a lookout check. In other words, they wouldn't be looking for you. They'd be looking for the bad guy and identify that. So that is there.

But if you're going to do a positive identification check, you either have to scan the photograph on the data page, or you have to read it from the chip.

Mr. HOSTETTLER. Thank you. I thank the gentleman.

Ms. JACKSON LEE. Mr. Chairman?

Mr. HOSTETTLER. Excuse me. The gentleman from Texas has the time.

Mr. GOHMERT. I'd yield to the gentlelady from Texas.

Ms. JACKSON LEE. I thank the distinguished—my new colleague, the distinguished gentleman.

Mr. Shaw, then, but the intent of getting a program biometric is, in fact—or part of the intent is to get that pure identification.

Mr. SHAW. That's correct.

Ms. JACKSON LEE. Is it not?

Mr. SHAW. That's correct.

Ms. JACKSON LEE. And I think that is important.

Mr. SHAW. Yes.

Ms. JACKSON LEE. Thank you.

Thank you, I yield.

Mr. HOSTETTLER. I thank the gentleman.

The Chair recognizes the gentlelady from California, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman. I think it's important for me to say that every Member of Congress is equally concerned about homeland security. We all are very hopeful and work toward—bring everything that we can to secure the homeland. So when we talk realistically about problems such as this one, and if we may not agree on whether or not there should be an extension of these countries, it's not because we are less concerned. It is because we are just realistic about what could and could not happen.

I'm looking at a Los Angeles Times article that says this—the last paragraph of the article says, "Meanwhile"—as it discusses changes in passports here and abroad. "Meanwhile, the European

Union hinted it might require visas of U.S. citizens if Congress refuses to extend an October deadline requiring machine-readable biometric passports for citizens of 27 visa waiver nations, mostly in Europe. It said many of its nations would not be ready with the passports by then."

This would be worse than a trade war if, in fact, the European Union decided that it would require of us what we're requiring of them. I think Mr. Berman pointed out that we could not meet that requirement should it be placed on us. So I think it's always very necessary, no matter how concerned we are about homeland security, that we recognize that there are some things that are just going to take time and work and effort. It seems to me there are a number of questions here—technology, retaliation, other kinds of issues.

So when I said earlier that based on my evaluation of this problem that I'm convinced that we will have to extend the deadline, it's because based on how things work and how this Congress works and how we work out problems is just not a question in my mind.

So I thought it would be important for me to just, number one, reiterate the fact that we're all concerned about homeland security, but I'm sure many of these other countries are concerned about their homeland security also. And I suspect everybody's working very hard to meet the deadline, but probably it will be missed. And it is at that point—at some point that we're going to have to come to grips with reality and simply extend the deadline in the interest of our relationships with the world and with the European Union in particular.

Having said that, I'm wondering from Mr. Veestraeten whether or not other countries have sought your country's help and assistance in developing their technology and if its technology that is offered can be accessed by other countries.

Mr. VEESTRAETEN. Yes, indeed, I've been contacted recently by Portugal, by Ireland, and by some other member states to see where we can better work together.

This being said, we all have our established relationships with national printing offices, national banks, with companies, so there is a different tradition at each different country for production of passports. Don't forget that the passport essentially remains a paper document. There is a chip in it now, but it essentially remains a very specific paper document with a lot of security features in the printing and in the paper. So that remains. It doesn't change. The way we all work, all governments work with those who produce the passports is different as a historic background. But I was indeed asked to see how we can better cooperate by the countries I mentioned.

Ms. WATERS. Thank you. And of the panel, have you found that most countries are working very hard to try and meet the deadline? Are they really attempting to do it? Is that true?

Ms. DEZENSKI. We would agree with that. We've been very active in the ICAO process, working closely with folks. And as I said earlier, I think there's been very much a good-faith effort to reach these deadlines and to do it as quickly as possible. And there's most definitely a sense of urgency in that process as well.

Ms. WATERS. Anybody else?

Mr. SKINNER. Congresswoman, we have not looked at that particular issue. In countries we did visit, however, we did determine that they were very diligent in their efforts to safeguard the integrity of their passport systems.

Ms. WATERS. What about you?

Mr. SHAW. Based on the experiences I've had with a number of countries, probably over a dozen, yes, they are. And they're encountering a range of different issues that they're facing, but they are all diligently working and trying to do one thing: make sure that the passport that is handed over at Homeland Security works. And that seems to be what they're trying to do.

Ms. WATERS. And, finally, if I may, Mr. Chairman, I know the red light is on, if you would grant me just another minute here.

Mr. HOSTETTLER. Without objection.

Ms. WATERS. Has there been a recommendation from anybody, any agency—Homeland Security, State Department, Immigration, anybody—to hold fast to this deadline and not to waver one bit that we can afford to extend the deadline? Have we heard that recommendation from anybody, anytime, anyplace, anywhere?

Ms. DEZENSKI. The Secretary is going to be coming up to talk to Chairman Sensenbrenner in a couple weeks, and I think we'll be able to be a little bit more specific. We have not at this point made any specific statements on changing the policy direction.

Ms. WATERS. Have you been advised by anyone to do that?

Ms. DEZENSKI. Not formally, no.

Ms. WATERS. Thank you all very much.

Mr. HOSTETTLER. The gentlelady's time has expired.

I make unanimous consent—I will allow the gentleman from Texas, who graciously gave up his time a few moments ago to myself and the Ranking Member, for 5 minutes for one last set of questions. And I very much appreciate the indulgence of the panel.

The gentleman from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman.

I was just curious, Mr. Veestraeten. Does the identifier you're using, does it have a biometric chip to it?

Mr. GOHMERT. Yes, indeed. Our passport contains—I think that the notes I deposited earlier this week contain some technical information. It contains a computer chip, and on the chip are stored all the data printed in the passport, like name, first name and so on, and a picture, a digitized picture of the bearer.

There is also room for another feature in the future, because you know that in Europe we have decided to go beyond the chip and the picture. We have decided with the second deadline, February 2008, to also include the second biometric feature. So this goes beyond the PATRIOT Act at the moment, and so there is another deadline we imposed on ourselves for further steps to be taken.

Mr. GOHMERT. Who produces the chip that you utilize?

Mr. VEESTRAETEN. It's a Phillips chip, as far as I know, but I'm not a specialist of the real technique. But the chip is Phillips. The antenna is a printed serigraphic antenna.

Mr. GOHMERT. Who produces the reader that you use that you've had no problems with?

Mr. VEESTRAETEN. The reader is a standard PDA, a pocket PC, and the reader antenna which is inserted is created by ACG, which is a company at the moment in Austria. It is produced in Austria.

Mr. GOHMERT. I see. Okay. Thank you. And I do appreciate you-all's testimony and your indulgence. But I do look at homeland security basically, to use the analogy, I mean, you're our police chief. That's your main job. We're looking to you to protect us. And I appreciate all the efforts that you will make on our behalf to do just that.

Thank you.

Ms. JACKSON LEE. Would you yield just for a moment?

Mr. GOHMERT. Yes.

Ms. JACKSON LEE. Ms. Dezenski, you said that—I just want to get a qualification. I know that the Secretary will be coming up, but you have—there is no pronounced policy right now in the Department of Homeland Security about not extending the Visa Waiver Program deadline.

Ms. DEZENSKI. That's correct.

Ms. JACKSON LEE. And so that means that as a witness here, you're also willing to accept, I assume, comment or insight from the affected persons and consult with State along with Members of Congress.

Ms. DEZENSKI. Absolutely, and that process is already underway.

Ms. JACKSON LEE. All right. Thank you very much. I yield back.

Mr. GOHMERT. She yielded back. Let me just say I also look at you as representing the Beauty, Ms. Liberty, and I hope you won't embrace the Beast. [Laughter.]

Ms. JACKSON LEE. Now, Mr. Chairman, I really have to have him yield back. [Laughter.]

The choice is between the Beauty and the Beast, and I hope that we'll accept the Beauty, which is to work with this problem for the betterment of our international relations and the homeland security, which we as Democrats and friends on the other side of the aisle have as one of our number one agenda items.

I yield back.

Mr. HOSTETTLER. And with that, we bring this Subcommittee hearing to a conclusion.

I would like to inform the witnesses that we will be following up with some questions to some of you. We would appreciate a timely response, within approximately 3 weeks, to have this added to the record. And all Members will have 5 legislative days to include extraneous remarks into the record, as well as questions for the panel members.

I want to once again thank all the members of the panel, especially you, Mr. Veestraeten, for being here and for taking time to help us, and this, as you can imagine from the participation, that your being here and your input is very valuable and will be extremely valuable as we continue to develop policy in this area.

Ms. WATERS. Mr. Chairman, I'd like unanimous consent to submit my statement for the record.

Mr. HOSTETTLER. Without objection.

Mr. HOSTETTLER. The business before the Subcommittee being completed, we are adjourned.

[Whereupon, at 2:59 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

RESPONSE TO CHAIRMAN JOHN HOSTETTLER'S QUESTION POSED TO MS. ELAINE DEZENSKI AT THE HEARING, SUBMITTED BY THE U.S. DEPARTMENT OF HOMELAND SECURITY

House of Representatives

Committee on the Judiciary
Subcommittee on Immigration, Border Security and Claims

Oversight Hearing on the October 2005 Deadline for Visa Waiver Program Countries to
Produce Secure Passports: Why it Matters to Homeland Security

Thursday, April 21, 2005

Supplemental Material for the Record

We respectfully request that the following supplemental information be inserted for the record in response to Chairman Hostettler's question.

Q: Do you know how many times you've had to do that, how many times you've had to inform ICE of that?

A: Since we began monitoring the issue, in January, 2005, CBP has found10 cases in which it appears that a reported lost/stolen passport was used and subsequently reported to ICE.

PREPARED STATEMENT OF THE HONORABLE F. JAMES SENSENBRENNER, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN AND CHAIRMAN, HOUSE JUDICIARY COMMITTEE

On September 11, 2001, the United States was attacked by 19 terrorists who flew planes into American landmarks, resulting in the largest single terrorist-related loss of American life in our history. The leaders of that terrorist attack either lived in Europe as resident aliens prior to the attack or traveled directly from Europe en route to the execution of this awful assault. Subsequent arrests in Spain, combined with examination of the terrorists' travels, have confirmed that the attacks were

planned in Europe, in countries enjoying Visa Waiver Program status. Zacarias Moussaiou, the "20th terrorist" who has just this week announced he wants to plead guilty to the terrorist charges against him, came to the U.S. from France with a French passport under the Visa Waiver Program. These sobering facts are no less relevant today than they were three years ago.

I authored the Enhanced Border Security and Visa Entry Reform Act of 2002 to address several of our Nation's vulnerabilities to terrorism. The need for the legislation was clear to everyone in Congress at the time, as evidenced by its virtually unanimous passage. The need for including the passport and visa requirements was not in dispute then, and should not be in dispute now.

One requirement of that Act, was that by no later than October 26, 2004, the governments of visa waiver program countries certify that they have programs to issue their nationals machine readable passports that are tamper-resistant and incorporate biometric identifiers that comply with biometric identifier standards established by the International Civil Aviation Organization. Because the 2002 ICAO standards seemed straightforward at the time, the only obstacle to Visa Waiver Program countries meeting the 2004 deadline was for ICAO to update standards for digital photographs of the facial images contained in passports, and possibly address some software and camera technicalities relating to how the photos could be read by machine standards for purposes of validation.

My goal in selecting the October, 2004, deadline was to push countries to act promptly to modernize their passports. Unfortunately, only a few countries took the deadline seriously, and for that I partly blame weak efforts by the Department of State and the Department of Homeland Security to convince the effected countries that we were serious.

The Border Security Act stipulated only that biometric identifiers and documents meet ICAO standards, and that the passport be "machine-readable." Congress, in passing the Act, anticipated that ICAO would establish reasonable, cost-effective standards which relied upon existing technology. That the ICAO would become enmeshed in new and unproven technology, and that the EU should choose an elaborate and expensive path to meet the requirement has led to consequences that are regrettable, but not insurmountable.

Visa Waiver Program countries have had since the spring of 2002, one year more than initially set, to move forward to produce passports meeting those requirements. Some Visa Waiver countries have acted promptly to initiate the necessary processes, while others delayed. Recently, I asked Visa Waiver countries to update me on their progress toward meeting the requirements. From the responses received thus far, it appears at least twelve countries will have a viable program in effect prior to the October deadline. In the order responses were received, these include: Germany, Ireland, New Zealand, Belgium, Australia, Italy, Singapore, Luxembourg, Slovenia, Sweden, the Netherlands, and the United Kingdom.

VWP countries failing to meet the deadline delays will impose burden on their citizens as well as costs on the United States, as our State Department will be required to staff up foreign posts to handle this visa demand. As I receive more letters, and further clarification on some of the letters received, I hope to find that all or nearly all of the Visa Waiver Program countries are moving forward quickly to meet the deadline.

QUESTIONS FOR THE RECORD SUBMITTED TO THE U.S. DEPARTMENT OF HOMELAND SECURITY BY CHAIRMAN JOHN N. HOSTETTLER

F. JAMES SENSENBRENNER, JR., Wisconsin
CHAIRMAN

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
RANKING MINORITY MEMBER

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

ONE HUNDRED NINTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

April 27, 2005

The Honorable Pamela J. Turner
Assistant Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Ms. Turner:

Thank you for attending the latest Subcommittee hearing on the Visa Waiver Program (VWP) and biometric passports. I and other members were disturbed by the revelation of so many cases of imposters using lost or stolen passports from visa waiver countries to successfully enter the United States. Similarly disturbing was the fact that so few of these cases were subsequently investigated and the alien apprehended. I would appreciate your ensuring that the appropriate offices respond in writing to the following questions, to be submitted for the record:

- How many times has Immigration & Customs Enforcement (ICE) sought to apprehend aliens known to have entered with bought, stolen, lost, or altered passports?

- What is the Department's assessment as to whether aliens who utilized stolen passports from the same batch of stolen passports found with individuals associated with al Qaeda and involved in the assassination in Afghanistan of Northern alliance leader Ahmad Shah Massoud may still be within the United States? (See DHS/OIG Report OIG-05-07, December 2004).

- What is the state of compliance by VWP countries with the October 2004 requirement that aliens arriving under the visa waiver program have machine-readable passports?

- When will all ports of entry be equipped with scanners to read the biometric features of the passports used in the Visa Waiver Program?

- Secretary Ridge assured the Committee in May 2004 that the Department of Homeland Security (DHS) would clarify the policy on actual program requirements for VWP countries so that the various governments know what is necessary to meet the October 26, 2005, deadline for issuing passports with biometric identifiers. When will the Department issue a policy statement?

- A report on the Visa Waiver Program and the basis for countries to meet the current Visa Waiver Program requirements was due at the beginning of 2005. When will that report be issued?

- Will the information obtained by DHS during its 2004 review of VWP countries be applicable to complete the certification of compliance or will a new round of passport procedure inspections be needed?

- Why did DHS create a "de facto" waiver of the machine-readable passport requirement through the use of parole whenever an alien presents a non-machine readable passport for the first time? What are the security risks of continued waiver?

- Please explain how DHS adequately prepared for the necessary equipment and procedural changes to compare the information secured on biometric passports with the visitor? Please explain what procedural changes will be required?

At the previous Subcommittee hearing, held March 10, on interior immigration enforcement resources, the Deputy Inspector General of the Department of Justice testified on a study (Report # I-2003-004) dealing with the removal of aliens issued final orders. One of the recommendations, which now falls to your agency (having current responsibility for detention and removal), was to "complete the current rulemaking entitled, *Requiring Aliens Ordered Removed from the United States to Surrender to the Immigration and Naturalization Service for Removal*." A copy of the Report and the proposed regulations are enclosed for your convenience. Please (a) indicate that your agency will comply with the recommendations of the Inspector General, (b) provide the status of these proposed rules, and (c) provide a timeline for finalization.

Hon. Pamela Turner
April 27, 2005
Page Three

Thank you for your cooperation in this matter. Please respond to all these inquiries within three weeks. If there are any questions, please contact Subcommittee Counsel Luke Bellocchi at (202) 225-5727.

Sincerely,

JOHN N. HOSTETTLER
Chairman, Subcommittee on
Immigration, Border Security, & Claims

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

The visa waiver program (VWP) allows nationals from 27 countries to enter the United States as nonimmigrant visitors for business or pleasure without first obtaining a visa from a United States consulate office. This facilitates international travel and commerce and eases consular office workloads.

The Enhanced Border Security and Visa Entry Reform Act of 2002 mandated that by October 26, 2004, the government of each VWP country would have to certify that it had established a program to issue machine-readable passports that are tamper-resistant and incorporate a biometric identifier. We extended that deadline to October 26, 2005, last year. The extension was necessary to avoid potential disruption of international travel and to provide the international community adequate time to develop viable programs for producing a biometrically enabled passport.

According to the State Department, only 14 of the 27 VWP countries expect to comply with the revised deadline. Brunei, Finland, Ireland, Portugal, Spain, Switzerland, and the United Kingdom expect to come into compliance several months after the deadline. Longer delays are anticipated by France, Japan, Denmark, Italy, Liechtenstein, and the Netherlands.

Most of the countries that expect to meet the deadline are small countries that have small passport production numbers and centralized production processes. Those with large passport production numbers are the ones having greatest difficulty in meeting the deadline. France, Japan, Germany, and the United Kingdom make up more than 80% of VWP travelers.

If the deadline is not extended, the VWP countries that fail to meet it will lose the privilege of participating in the program, and the nationals of those countries will need visas to enter the United States. The State Department has estimated that this would result in a sudden need to process millions of additional visas, which would impose a severe challenge on its resources.

I am concerned about the effect that even a temporary disruption of the visa waiver program could have on the international tourist industry. In 2002, approximately 13 million international visitors entered the United States on the Visa Waiver Program. They spent nearly $40 billion and supported the jobs of hundreds of thousands of American workers. A disruption to the Visa Waiver Program would discourage international visitors. Many of them would choose to travel to other international destinations.

I am particularly concerned about the effect that this might have on the State of Texas. In the year 2000, Texas received revenue from the international tourist industry that totaled $3,751.3 million. This included $410.6 million on public transportation, $111.1 million on automobile transportation, $1,029.2 million on lodging, $731.4 million on food services, $320.2 million on entertainment and recreation, and $1,148.9 million in general trade.

Also, the technology for the biometric feature needs to be fully developed and tested before it is put into use. I am afraid that rushing the VWP countries into compliance could result in passports that have unreliable biometric identifiers, which would not provide the expected increase in our security.

It is not a crisis if we have to permit some short extensions to the present deadline. The biometric passport is important, but we have other security measures that are already in place. Since September 30, 2004, all VWP travelers entering the United States have had their fingerprints electronically collected and compared against watch-lists through the US- VISIT program. The Advanced Passenger Information System (APIS), provides information on international visitors before they arrive. And these efforts are augmented by United States law enforcement and intelligence operations.

Nevertheless, I want the biometric requirement to be met as soon as possible. I would only favor granting additional extensions on a case-by-case basis, and I would expect the countries requesting additional time to support their requests with a detailed time table for achieving compliance within the time requested.

Thank you.

LETTER FROM THE TRAVEL BUSINESS ROUNDTABLE, TRAVEL INDUSTRY ASSOCIATION OF AMERICA, AND U.S. CHAMBER OF COMMERCE, SUBMITTED BY THE HONORABLE SHEILA JACKSON LEE







April 21, 2005

The Honorable John Hostettler
Chairman
Subcommittee on Immigration, Border Security and Claims
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable Sheila Jackson Lee
Ranking Member
Subcommittee on Immigration, Border Security and Claims
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman and Ranking Member:

On behalf of the U.S. travel and tourism industry, we urge your Subcommittee to support a one-year extension of the October 26, 2005 deadline for including biometric elements in passports of Visa Waiver Program countries. We appreciate your leadership in holding the oversight hearing on April 21 to address this critical deadline and ask that you include our letter in the hearing record.

Biometric passports are an important element in securing our borders. Definitive identification of international visitors through biometrics will allow U.S. inspections to admit legitimate travelers with greater confidence. This will increase security as well as lessen wait times at inspection.

The U.S. travel and tourism industry is grateful for the leadership of the House Judiciary Committee in working with the Departments of State and Homeland Security, and the governments of the 27 Visa Waiver Program countries, to ensure all parties are advancing their programs to meet this important security goal. Without the strong guidance of the House Judiciary Committee, it is very likely that the Visa Waiver Countries may not have progressed as far as they did as fast as they did. In both individual and group meetings, the travel industry has urged Visa Waiver countries to move as expeditiously as possible to meet these deadlines.

Reportedly, a number of important Visa Waiver Program countries will not be able to comply with the October 26, 2005 deadline. Additionally, our government does not have the ability to meaningfully use the biometric information contained in the passports. The Department of Homeland Security currently lacks document readers that can read all of the 27 prototype biometric passports. Without a "universal" passport reader, Homeland Security will receive no biometric security advantages for those passports it cannot read.

The U.S. travel and tourism industry is dedicated to supporting the federal government's work to help secure this nation from further terror attacks. The travel industry strongly supports the US-

VISIT Program. This program collects biometric finger scans of international visitors regardless of the type of passport they carry. With the US-VISIT program in place, Congress can extend the deadline and have Homeland Security continue to collect biometric information on Visa Waiver Program travelers.

The travel industry has advocated that Congress and the Administration take actions and set policies that make our homeland more secure while at the same time not creating real or perceived barriers to legitimate travel to the United States. Securing the homeland is indeed the top priority. However, we are confident the U.S. government can achieve enhanced security goals while at the same time facilitating legitimate international travel to the United States.

Uncertainty in the marketplace will only discourage travel to the U.S. and could have a crippling effect on future travel bookings for this coming fall and beyond. The sooner Congress acts to statutorily extend this deadline, the sooner we can reassure these important tourism trading partners and the more than 13 million Visa Waiver Program visitors that they can continue to travel uninterrupted to the United States.

On behalf of the travel and tourism industry, we would like to thank you again for holding this important oversight hearing. We urge you to introduce and advance legislation through the U.S. Congress in an expeditious fashion to extend the biometric passport deadline by one year.

Sincerely,

Travel Business Roundtable
Travel Industry Association of America
U.S. Chamber of Commerce

cc: Hon. F. James Sensenbrenner, Jr., Chairman
Hon. John Conyers, Jr., Ranking Member
Committee on the Judiciary
U.S. House of Representatives

PREPARED STATEMENT OF THE HONORABLE MAXINE WATERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, our Visa Waiver Program needs vast and extensive improvement. In today's climate of terrorism, our ports of entry and the immigrants allowed into the country through the Visa Waiver Program, needs to be rigorously modified and monitored.

When evaluating the Visa Waiver Program, procedures for ascertaining INS's ability to account for nonimmigrant overstays, stolen passports from Visa Waiver Program countries, falsified passports, and INS's ability to correctly and consistently check applicants against the Terrorist lookout system or Watchlist data, seem chaotic and lax. This is not acceptable in today's climate.

Mr. Chairman, the Visa Waiver Program does bring in a significant financial gain to America's tourism industry, hence boosting America's overall economy, but I'm not sure those financial gains are worth the threat of terrorism and illegal activity.

I look forward to hearing from today's witnesses to learn more about the Visa Waiver Program and how its procedures have progressed. For it is a valuable program, if we can rigorously and thoroughly protect our ports of entry and integrate procedures that will effectively prevent criminals and terrorists into America.

I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE ELTON GALLEGLY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you for holding this hearing, Mr. Chairman.

I introduced legislation in the 107th Congress that included a requirement that all visa waiver countries redesign their passports to be machine-readable and contain biometric identifiers as a condition of their continued participation in the visa waiver program. My bill was the model for such requirements included in the "Enhanced Border Security and Visa Entry Reform Act of 2002," that are now the subject of this hearing.

I am disturbed that our visa waiver partners did not meet the original deadline and to this day have not implemented the biometric and machine readability requirements. I am particularly concerned about how the failure to meet this deadline will impact the national security of the United States.

Though I understand that there are constraints, and coordination on a worldwide level is not a simple matter. However, I wish to implore our visa waiver partners to treat security improvements with the utmost urgency.

Again, thank you for holding this hearing, Mr. Chairman. I look forward to hearing from the witnesses about the reasons for the delay and, most importantly, when we can expect them begin to issue biometric, machine-readable documents.

I yield back my time.

