AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–910

BIOMETRIC PASSPORTS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 15, 2004

Serial No. J–108–82

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

28–598 PDF WASHINGTON : 2006

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

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
LARRY E. CRAIG, Idaho
SAXBY CHAMBLISS, Georgia
JOHN CORNYN, Texas

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

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	18
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	1
prepared statement	73
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	84

WITNESSES

Cantwell, Hon. Maria, a U.S. Senator from the State of Washington	2
Harty, Maura, Assistant Secretary for Consular Affairs, Department of State, Washington, D.C.	7
Hutchinson, Asa, Under Secretary, Border and Transportation Security, Department of Homeland Security, Washington, D.C.	5

QUESTIONS AND ANSWERS

Responses of Maura Harty to questions submitted by Senators Kyl and Chambliss (Senator Chambliss submitted a question on behalf of Senator Sununu)	24
Responses of Asa Hutchinson to questions submitted by Senators Kyl, Leahy, and Chambliss (Senator Chambliss submitted a question on behalf of Senator Sununu)	58

SUBMISSIONS FOR THE RECORD

Cantwell, Hon. Maria, a U.S. Senator from the State of Washington, prepared statement	66
Harty, Maura, Assistant Secretary for Consular Affairs, Department of State, Washington, D.C., prepared statement	68
Hutchinson, Asa, Under Secretary, Border and Transportation Security, Department of Homeland Security, Washington, D.C., prepared statement	75

BIOMETRIC PASSPORTS

TUESDAY, JUNE 15, 2004

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:07 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch, Kyl, Sessions, Chambliss, and Feinstein.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. Good morning and welcome to the hearing on biometric passports. Since last fall, this Committee has held eight oversight hearings that substantially focus on our Nation's efforts to prevent and respond to terrorism on American soil. The purpose of these hearings is to make sure that the United States government is taking every possible step to protect this country and its citizens from the evil intentions of terrorists and that every available resource is focused toward that end. Implementation of the biometric passport program will be an important resource in our fight against terrorism and we should be vigilant in our efforts to fully implement this program.

Today, we focus our attention on the biometric passport requirement set out in the Enhanced Border Security and Visa Entry Reform Act. This legislation provided crucial tools to tighten immigration procedures and close loopholes in our border security which were, in my view, of paramount importance after the catastrophic attacks this Nation suffered on September 11, 2001. I was proud to be an original cosponsor of this legislation and am disappointed that more than 2 years after its enactment, we are faced with the reality that the biometric passport deadline of October 26, 2004, will not be met.

Now, I understand that when we called for the development and inclusion of biometric passports, the fundamental technologies were not yet mature. Nonetheless, many of us believed that we needed cutting-edge technology in order to thwart the increasingly sophisticated terrorists. This mandate has presented difficult challenges for the many capable scientists and technicians who have dedicated themselves to this particular effort.

But we can and must demand that the countries who participate in the Visa Waiver Program begin producing and distributing these passports. Every day that biometric identifiers are not utilized, our

country and its citizens are more vulnerable to terrorist attack. So I strongly urge the Department of State and Department of Homeland Security to work with these participating countries in the upcoming months to establish an interoperable system for biometric passports.

I have spoken to Secretary of State Powell concerning the importance of the biometric passport issue, and during his testimony before this Committee last week, Secretary Ridge also emphasized the importance of this issue. Both of these men, whom I highly respect, have requested a 2-year extension to the current biometric passport deadline of October 26, 2004. However, I am concerned with the national security implications that such a lengthy extension may cause. Frankly, I would like to require why a 1-year extension is not feasible for implementation of the biometric passport program.

As this deadline extension has implications on our National security, I hope that our witnesses today can fully explain to this Committee the reasons for extending the current biometric passport deadline. I will be interested in those reasons, and, of course, I understand Chairman Sensenbrenner in the House feels somewhat strongly on this issue. On the other hand, I want to accommodate our public leaders who have these difficult jobs and do what I can to always be of assistance to them, and I am sure Chairman Sensenbrenner feels the same way.

Today, the Committee will hear from two panels of witness testimony. The first panel consists of testimony by Hon. Maria Cantwell, Senator from the State of Washington. I would like to welcome Senator Cantwell, who was a cosponsor of the Enhanced Border Security and Visa Entry Reform Act. I know that she feels strongly about this issue and I want to thank her for taking time to appear before the Committee.

I might mention that over the weekend, I did see your former boss, Rob Glaser of Real Networks and he said to say hello to you.

Senator CANTWELL. Thank you.

Chairman HATCH. The second panel consists of testimony by Hon. Asa Hutchinson—Secretary Hutchinson, we are really honored to have you here—Under Secretary for Border and Transportation Security at the Department of Homeland Security. And, of course, we have Hon. Maura Harty, the Assistant Secretary for Consular Affairs at the Department of State. We equally welcome Ms. Harty. I welcome both of you good people to our Committee and appreciate your testimony on this very, very important issue at this very, very important time.

With that, I will insert the ranking member's statement into the record and we will interrupt when he comes, but we will turn to Senator Cantwell until then.

[The prepared statements of Senators Leahy and Hatch appear as submissions for the record.]

STATEMENT OF HON. MARIA CANTWELL, A U.S. SENATOR FROM THE STATE OF WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman, and thank you for the opportunity to appear before the Committee. As a former member of the Judiciary Committee, I miss my time being here on

the Committee and the lively and spirited and intelligent debate that this Committee provides, so—

Chairman HATCH. That is an interesting comment for somebody who has the experience you have. We miss you on this Committee, too. We wish you were back.

Senator CANTWELL. Thank you, Mr. Chairman. I appreciate the opportunity to testify this morning because the need for greater border security became a glaringly evident issue in the Northwest in 1998 when Ahmed Ressam, a terrorist trained at one of the Osama bin Laden training camps in Afghanistan, was arrested shortly after crossing the Canadian border at Port Angeles, Washington. Explosives and other bomb materials were found in the trunk of Ressam's car. Ressam's plan was to head to Los Angeles and blow up LAX airport. But thanks to the hard work of Diana Dean, the U.S. Customs Inspector, the terrorist was apprehended.

This frightening incident made it clear, the vulnerabilities we face along the porous Northern border and the vulnerabilities that became even more concerning after the September 11, 2001, terrorist attacks. But the Ressam case raised important questions about our international standards.

Ressam began his journey on a French visa, leaving Algeria and landing in Versailles. Ressam came to the United States after creating a trail of fraudulent documents on his journey from Algiers to the United States, first obtaining a French passport on the basis of a fake French birth certificate. He then entered Canada under his own name, seeking refugee status. While living in Canada, he used a false baptismal certificate to obtain a Canadian passport under an alias.

An international biometric standard for visas would have identified Ressam the first time he tried to enter France. The identification would have become traceable when he entered Canada and then the United States and could have been more easily stopped. Obviously, we can't always count on the good work of our Border Patrol to stop every individual, so this information is paramount.

That is why I worked with you, Senator Hatch, and Senator Leahy, in the Patriot Act to establish the technology standard for the U.S. visa program. Those provisions, Section 403(c) of the Patriot Act, called for a technology standard to facilitate a comprehensive screening of visa applications at our overseas consulates and to access the necessary law enforcement, watch list, and intelligence information at our consular offices and at border crossings, and the verification of identifying persons crossing our borders being the same people who obtained the travel documents.

In the Enhanced Border Security and Visa Entry Reform Act of 2002, I also worked with this Committee and Senators Kennedy, Feinstein, Brownback, and Kyl to include in Section 603 a requirement that the Department of Homeland Security coordinate with this same technology requirement in the Patriot Act to work with Canada, Mexico, and the 27 visa waiver countries. This would implement standards for visa programs that could be compatible with those adopted in the United States.

More simply said, we must recognize that we need international cooperation to be successful with our visa technology standard. It must be compatible with our own. This would enable us to catch

the Ressams of the world at a sooner place in time, before they got to the United States.

The problem begins in the United States. The requirement of the visa technology standard, like the passport standards, have not been met and that is the subject of this hearing. Congress required that the visa standard be set by 2003. In a report issued in November of 2002, the National Institute for Standards and Technology, the standards body for creating the standard, recommended a dual biometric for visas, fingerprints and facial recognition.

With the U.S. VISIT program, the Department of Homeland Security has begun to implement a national biometric program using dual biometrics, but the biometrics chosen do not allow for searching FBI or Interpol databases, and perhaps that can be commented on later, but that is my understanding. More analysis should be done on what is the appropriate standard to maximize international cooperation and international information.

The Department of State and Department of Homeland Security must make it a priority to establish U.S. standards and to work with the international standards setting organization. This ISO, which is a network of national standard institutes from 148 countries and the International Civil Aviation Organization, can work to help us implement these standards.

We need to stop terrorists before they are at our borders. In fact, we should be working first, which I believe the State Department will testify, in those seven states that the Department has listed as terrorist states in establishing these visa technology standards. Then we must set a priority in working with the 27 waiver countries, that they also adopt these standards so that they again can make sure that people, as in Ressam's case, starting in a country, then entering one of those 27 waiver countries and then coming to the United States, are stopped at an earlier point in time.

The 19 hijackers that perpetrated the attack on the United States on September 11 had submitted 24 visa applications, receiving 22 tourist visas and one student visa. The 19 entered the United States a total of 33 times before flying airplanes into the Twin Towers and the Pentagon. We need to do a better job at getting the technology and securing our visa process with these international countries.

I am glad that the Committee is taking a closer look at this issue. I look forward to hearing the testimony of both the agencies that are presenting today and hoping that this visa standard can be met in the near future. There are obviously significant challenges to meeting that standard and there are concerns about this delay. I am suggesting just one issue that the Committee might consider, and that is that we continue to have a six-month update by this Committee until we actually get the standard in place and encourage the Committee to continue to work on the oversight as it relates to setting an international standard that hopefully can maximize the use of the Interpol data so we can catch these people, as I said, before they reach our borders.

Thank you, Mr. Chairman.

[The prepared statement of Senator Cantwell appear as a submission for the record.]

Chairman HATCH. Thank you. I appreciate your testimony. I know you are an expert in this area and it means a lot to us that you would take time to come see us.

Any questions from anybody?

[No response.]

Chairman HATCH. With that, we are glad to have had you here.

Senator CANTWELL. Thank you, Mr. Chairman.

Senator SESSIONS. Senator, I thank you very much for coming. You indicated that—I don't know if you want to talk about it now—it is important, your comment that FBI and Interpol databases may not be accessible under some of the proposals that are out there. I think that is real important. Do you agree?

Senator CANTWELL. Yes, I do, and I think that there is more progress being made by companies working on an international standard with that ISO organization, and the question becomes, do we have a standard that we set in the United States that is compatible in accessing all that information. While today we might only want to access, say, our FBI files, it would be an interesting question whether Mr. Ressam, starting in Algiers, would have been in the Interpol database already on something else. Obviously wanting to stop people at point of origin as opposed to the point of entry into the United States would be a better process, so getting that standard.

Chairman HATCH. Thank you, Senator Cantwell.

Senator CANTWELL. Thank you.

Chairman HATCH. We really appreciate your taking time from what we know is a busy schedule.

Senator CANTWELL. Thank you, Mr. Chairman.

Chairman HATCH. Thank you. If we could have our good friend Asa Hutchinson, Under Secretary for Border and Transportation Security, Department of Homeland Defense, and Hon. Maura Harty, who is the Assistant Secretary for Consular Affairs in the Department of State, come to the table. We appreciate having both of you here, and again, I would like to welcome both of you.

Secretary Hutchinson is a former member of Congress with distinguished service on the House Intelligence and Judiciary Committees. I also understand that Secretary Hutchinson, at the age of 31, was appointed U.S. Attorney for the Western District of Arkansas. At that time, if I recall it correctly, you were the youngest U.S. Attorney in the country.

We also welcome Secretary Harty, who has honorably served our country for over 20 years in the Foreign Service and was a former U.S. Ambassador to the Republic of Paraguay. We admire your dedication, Ms. Harty, and your service to our country and look forward to your testimony here today.

Under Secretary Hutchinson, you can proceed with your opening statement.

STATEMENT OF ASA HUTCHINSON, UNDER SECRETARY, BORDER AND TRANSPORTATION SECURITY, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. HUTCHINSON. Thank you, Chairman Hatch, distinguished members of the Committee. It is a pleasure to appear before you to discuss the Department's commitment to enhance the security of

our citizens, our international visitors, and our Nation through the use of biometric technology. It is a pleasure to appear with Maura Harty, my good friend and partner in this endeavor from the Department of State.

I would emphasize that it is important that we work through our partnership in the international community to integrate the biometric technology into passports and travel documents in accordance with international standards, best practices, and our own statutory requirements. The involvement and cooperation of the 27 countries that comprise the visa waiver program are critical to establishing an effective system for managing the entry and exit of millions of travelers each year.

The use of biometrics, including digital finger scans and photographs, is consistent, in my judgment, with the values and character of our Nation and our commitment to enhance security while facilitating legitimate trade and travel, respecting individual rights and privacy, and maintaining positive relations with our allies. Also, it helps us to effectively use our taxpayer dollars.

For that reason, I would like to reiterate the administration's request for a 2-year extension of the deadline for the visa waiver program countries to issue machine-readable passports. As you known, the program enables citizens of certain countries to travel to the United States for 90 days or less without obtaining a visa. And while visa-less travel encourages travel and trade with our allies, it also makes the program attractive to those who wish to avoid visa security checks conducted at our consular offices and even would be an invite for terrorists.

Congress has addressed this security vulnerability by requiring visa waiver program countries to issue tamper-resistant machine-readable passports, including biometric identifiers, in accordance with international standards. While most countries have initiated programs to meet the current deadline, very few, if any, countries will be in a position to issue passports in that time frame, and this is due in most cases not to a lack of will or commitment to enhanced security, but a result of technical or scientific challenges.

The Department of Homeland Security must also implement a system to process those passports by the October 26 deadline. We will not be in a position to biometrically compare and authenticate those travel documents due to immense technical challenges, including the need to test and develop a system that will rely upon a single type of machine reader to process passports from 27 countries. We prefer not to develop a reader or multiple types of readers for different passports that are issued by the 27 different countries.

Based upon information provided by these countries as well as the Department of State's experience, we believe that all countries can be compliant by November 30, 2006, and it should be a hard and fast deadline. Extending this date will also give the Department enough time to rigorously test the equipment and technology, and it is important, I believe, for us to get this process right the first time and not to spend additional time and resources to correct mistakes that might have been avoided.

During this time, we do need to enhance security, and for that reason, we are expanding our U.S. VISIT enrollment to include visitors under the visa waiver program beginning in September. As

you know, the U.S. VISIT system, for the first time in our country's history, allows us to biometrically confirm the identity of foreign visa travelers at our ports of entry. We believe processing these visitors under U.S. VISIT enhances our security, and by expanding it to visa waiver countries gives us some additional security capabilities.

It allows us to, through the biometric check, to check their identity against lookout databases that we have available. It also allows us to freeze the identity of the traveler and tie that identity to the travel document. It allows us to determine whether the traveler complied with the terms of his or her admission, previous admission, and in using that identity. We can collect arrival and departure information of travelers and update their records and their immigration status while they are in the U.S. We can determine if they have overstayed their visas. And obviously, we can give checks of their biometrics and biographic information against additional security databases that we have to assure that they are not a threat to the United States.

Since we implemented this on January 5, we processed over five million visitors. We have matched over 579 persons against criminal databases and prevented more than 196 known or suspected criminals from entering the country. Adding the visa waiver program countries will add an additional 13 million visitors to the system. I believe that we can do that successfully. We have that in plan by September 30. We believe the 2-year extension will be helpful for us to meet our mutual objectives of security, cooperation with our allies, and an appropriate use of the taxpayers' dollars.

Thank you, Mr. Chairman.

Chairman HATCH. Thank you, Secretary.

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

Chairman HATCH. Ms. Harty, we will take your testimony.

STATEMENT OF MAURA HARTY, ASSISTANT SECRETARY FOR CONSULAR AFFAIRS, DEPARTMENT OF STATE, WASHINGTON, D.C.

Ms. HARTY. Thank you, Mr. Chairman, for the opportunity to testify today on the administration's request for a 2-year extension of the 10/26/04 deadline for inclusion of biometric features in passports issued by countries which participate in the visa waiver program. I also would like to report on State Department's progress in developing our own biometric passport.

The inclusion of biometrics in international travel documents to verify the identities of prospective travelers to our country is a critical step in improving our border security and as part of our collective effort to combat terrorism. Naturally, the inclusion of biometrics in our passport is not the only step we are taking to enhance the security of our borders. We are working hand-in-hand with our friends and colleagues at the Department of Homeland Security to improve a multi-layered and interlocking system of border security through greater information sharing among agencies and with the VWP governments, through enhanced passenger screening and pre-clearance measures, and through DHS's recent

decision to expand the U.S.–VISIT program to include visa waiver country travelers.

State and DHS are currently in the middle of a Congressionally mandated biennial review of the VWP countries, assessing their compliance with the terms of the program and the criteria established by Congress. At all visa adjudicating posts overseas, consular officers have pushed our borders out beyond physical limits as a nation. They are seeing people well before they ever begin their travel, and through our Visa Viper programs overseas, every element of an embassy contributes to reporting on anyone who might be in a position to do this country harm.

As you know, the Enhanced Border Security Act (EBSVERA) established 10/26/04 as the deadline by which travelers entering the U.S. under the Visa Waiver Program must present passports that incorporate biometric identifiers that comply with the ICAO standards. In May of 2003, ICAO decided to make facial recognition encrypted on contactless chips the globally interoperable, standard passport biometric. Thus, visa waiver program countries had 17 months from that date to bring a biometric passport from design to production.

EBSVERA does not provide a waiver of that provision, and few, if any, of those countries will be able to meet this legislatively mandated deadline. Although the countries are committed to deploying biometric passports, they are encountering the same technical difficulties and scientific issues that we have encountered.

The challenge given the international community by the Congressional mandate is a daunting one. There are complex issues with which we are well familiar, including the security of the passport data on the contactless chip and the international interoperability of readers and biometric passports, which we and our VWP partners have continued to work through together.

In May of 2004, ICAO established the technical standards for the interoperability of contactless chips and passport readers at ports of entry and the technical specifications for protecting passport data from unauthorized use. As a result, manufacturers can now begin producing passport readers that will be able to read multiple chips. Each country can now begin to do their program and put their passports together and test them in real world scenarios.

Now that the questions of global standards and interoperability have been laid to rest, we and the VWP countries can begin full development and deployment of our respective programs. Given the time that it has taken to resolve these technical complex issues, as I have said, few of the visa waiver countries, if any, will meet the deadline. In fact, it is not a question of ill will. It is very much a question of difficult science.

Although the legislative requirements do not pertain to the U.S. passport, we recognize that in our roll as leaders, we would or should do the very same thing and lead the way and demonstrate that this passport technology that is being required of them would be something that we would also engage in, and as I have mentioned earlier, we have run into the same problems that they have.

In regard to our own progress, we expect to be able to produce the first operational biometric passport this December. It won't be en masse, but we will have one by Christmas here in Washington.

We will then expand our program to official and diplomatic passports so that we have a sizeable number of passports to use as we sort of work through the program and make sure that our technology is intact and functional. We will then expand it more broadly in February of 2005 to our Los Angeles passport agency and we will work with Australia and the travelers themselves to make sure that these passports are, in fact, interoperable in every way.

Given our own experiences with respect to building a biometric passport program, sir, we believe that there are compelling reasons to extend the deadline to November 30, 2006, as the administration has requested. Failure to extend the deadline will have some serious consequences for the country as well as the Department of State, and we can certainly go into those, sir, as you so desire.

I would like to add to what Under Secretary Hutchinson has already said and to encourage the Committee to please consider the 2-year deadline that we have previously requested. I thank you for your time.

Chairman HATCH. Thank you so much.

[The prepared statement of Ms. Harty appears as a submission for the record.]

Chairman HATCH. Mr. Secretary, it is my understanding that the chosen biometric for this program is facial recognition, whereby a biometric photo is stored in a chip. The chip is then embedded in the individual passport. Now, I understand that this biometric standard was adopted by the International Civil Aviation Organization. I want to ask you just two questions.

Number one is, how reliable is this facial recognition biometric? And number two, does the chip have the ability to take on other biometric recognition features, such as fingerprints or any other, should the visa waiver countries choose to implement additional features for more enhanced security in the future?

Mr. HUTCHINSON. Thank you, Mr. Chairman. You are correct that ICAO, the International Civil Aviation Authority, did meet in May and set the standard, where we are grateful that they acted quickly after some international pressure to move in this direction.

You asked about the reliability of the current standards and the chip technology. First of all, the facial technology is not fully developed. It is sufficient for one-to-one matches so that you can use it to confirm identity, which is the overarching purpose of this initiative. It is not sufficient in accuracy to do a one-to-many match which gives you the capability through facial recognition to check databases. We are hopeful that that technology will improve as time goes on.

In addition, the chips have a lifespan currently of three to 5 years. As you know, in many instances, the passports are issued for six to 10 years. So right now, you will be adding a chip on there that has a shorter life span than the life of the passport itself, and this is again an area that we hope that industry will be able to improve their technology in reference to.

So we believe that we have standards that are well set, but we thought we had the standards well set a year or so ago and we recognize after testing that they were not sufficient. They came back and redefined those. We hope that the testing this time will show that everything is appropriate and ready to move forward.

Chairman HATCH. I know you are aware that just yesterday, the House passed a 1-year extension for the full implementation—full implementation of the full biometric program, or passport program. Now, you both have requested that this should really be 2 years. The Secretary of State made that case to me, as well, because of the technological challenges which you are outlining here today.

Are both of you saying that it is impossible to fully implement the program within the 1-year time limit that the House has set? Maybe, Secretary Harty, you would want to comment on that.

Ms. HARTY. I appreciate the question, sir. While I regret having to say that something is impossible, we have been told by almost all of the countries that they cannot get it done within a year. As I have already admitted, in our own program, we will get a passport done, a small number of passports done by the end of the year. But to go into mass production simply isn't possible in a 1-year time frame.

One of the things that we are very concerned about is that we truly would like to measure twice and cut once, that we would truly like to also be good stewards of our programs and our shared responsibilities for border security, but also taxpayer dollars. We would like to get it right and we have heard this over and over again from our VWP partners. We would not like to rush into getting it wrong.

Chairman HATCH. I know you have tried hard, really hard, to put this together, but how receptive are the visa waiver countries to our efforts to implement this program in an expedient manner? Are there any countries that have given you resistance to accomplishing this?

Ms. HARTY. No, sir. I don't think there is resistance at all. There is a tremendous "can do" spirit. We have seen it at ICAO. We have seen it at G–8. We have seen it in multiple international fora. We bring the visa waiver country embassies into the State Department all the time and talk through this. There is a tremendous desire to do it, and I think that the events in Spain of March 11 only punctuated the need to do just exactly this kind of thing.

And it is not restricted to the visa waiver countries, sir. We are very, very regularly approached by other countries who do not yet have machine-readable passports who also want to increase and enhance the validity and safety and security of their own documents. This is a tidal wave of good will. But the science has proven more difficult than we realized, as Under Secretary Hutchinson said.

Chairman HATCH. My time is up, but Secretary Hutchinson, you indicated you wanted to talk about that?

Mr. HUTCHINSON. Mr. Chairman, I think that Ms. Harty is correct that the countries are willing to proceed down this path, and some with great enthusiasm. Others, as we have gone through the assessments of who should be renewed for the visa waiver country program and where they are in the level of compliance, we look at how developed their program is in this regard and some of them, yes, we have a program which is primarily a plan to move forward when the standards are set. So there are varying levels.

I think the leadership of the United States has been essential in this arena and the Congress of the United States, and I think your

original question was whether anybody could—is it possible to do it within a year. Australia has taken the lead on that and really been aggressive in this arena and we are entering into testing with them, with Australia, New Zealand, Japan, and Germany. But the testing pattern is, like, next June. So that is a very short time frame for procurement after a June couple-month test. Even the most aggressive would have a difficult time doing it within 1 year.

Chairman HATCH. Thank you. I am going to turn to Senator Chambliss, and I am going to ask Senator Chambliss if you will continue to chair the hearing and follow up with the rest of the Senators here. You might want to take this chair here.

Thank you. I appreciate both of you coming.

Senator CHAMBLISS. [Presiding.] Thank you, Mr. Chairman, for calling this hearing on an issue that is critically important, not just to the United States but to 27 other countries, as well. Both you Secretaries, we appreciate your diligent work on this issue.

Secretary Hutchinson, as you know, myself along with several other Senators on this Committee have introduced legislation to extend the time frame for the implementation of these new biometric visas by 2 years. I know there are some valid reasons why, from a homeland security standpoint, that you have requested it—you, as a part of the administration, have requested that. Let me ask you two questions in that regard.

First of all, can you explain the various security measures, such as machine-readable passports, the passenger manifest agreement, and the lost and stolen passports database, that will essentially fill the gap as biometric passports are being implemented.

And secondly, I know you are aware of the Inspector General's report that has recently come out and has been somewhat critical of this process. Would you tell us what steps you have taken to ensure the overall security program since the Inspector General's report came out, please.

Mr. HUTCHINSON. Thank you, Senator Chambliss. In reference to the Inspector General's report that was on the visa waiver program and the capability, really, of the Department of Homeland Security to conduct the assessments, really, at the time that report was issued, it was really outdated because many steps had been taken in the interim and it was not very timely.

We have submitted to the Inspector General, I presume with a copy to the Senators that have inquired, our responses in detail to the recommendations that were made. One of the recommendations, for example, was that there be a responsible program office in the Department. That has been established within my directorate.

Secondly, they recommended that visa waiver countries be a part and enrolled in U.S. VISIT, our biometric check. That has been done. It is being done by September 30.

And so I believe those have been addressed. We have a very vigorous program. Our goal is to have all the assessments done by September 30. We are on target to do that. We have completed, I believe, well over half of the site assessments, working with the Department of State. So that review is in place.

In addition, of course, we are continuing to enhance our security capabilities overall, from the manifest checks on the flights. We

have an initiative with Interpol and our European colleagues on lost and stolen passports and utilizing Interpol as a database for exchange of information on lost and stolen passports. We have those also bilaterally with the different countries so that we have access to that information.

So we are continuing to enhance security even through our visa waiver country programs while we are continuing the assessment as to whether they should continue in that program.

Senator CHAMBLISS. Ms. Harty, do you have any additional comments along those lines?

Ms. HARTY. Thank you, sir. I agree with everything that Under Secretary Hutchinson just said. The advance passenger screening, machine-readable passports, which will all be required by this October, PNR, sharing of lost and stolen passport data are all things that add to what we are aiming for, which is a depth of security. This is like an onion that we are building rather than peeling, and as many ways as we can add layers of that onion and increase the degree of scrutiny which as a Government we apply to travelers, as well as the degree of difficulty to a maleficent traveler, is what we are working on every day together.

I would also like to add that in regular conversations with our VWP allies, they agree with those aims and goals. And so as we scrutinize our systems, so are they doing the same thing as they look at how they issue passports to their own nationals, visas and those kinds of things.

Senator CHAMBLISS. Have you given the 27 countries benchmarks to which they must comply by a certain date, and if so, how are they progressing on those benchmarks?

Ms. HARTY. We have a series of benchmarks, sir, that we have developed. It is a rather lengthy list, but we haven't put times to it. We haven't put specific dates to it. But we would go back to them quarterly to make sure that they know what the benchmarks are and so that we could see progress therein, yes, sir.

Senator CHAMBLISS. Okay. If we extend this by a year versus the 2 years, is the likelihood that we are going to be back here pretty high, Senator Hutchinson?

Ms. HARTY. We wouldn't want to be doing that, sir. As we talked last year, 1 year ago, about the machine-readable passport issue, which did have an attendant ability by the Secretary of State to extend, we said last year that we would go back to the countries once with respect to the machine-readable passport requirement and we would not come back to the Senate and ask for another extension. We did not. We will not, even though there may be one country that has a problem with that. We were clear. We set a benchmark, and we would not back down from that. I would assume that we would be doing the same thing with this, sir.

I think that we can see, not only through the benchmarks and the process that we will go through over the next, I hope, 2 years to get everybody on board on the program, that there won't be any surprises, that countries will communicate with us as we will with them and we will know every step of the way. We will also be able to make better judgment on where to expend our resources with respect to any country that might not be able to, despite the in-

creased 2-year deadline, make it. They will just need visas after that, sir.

Mr. HUTCHINSON. Mr. Chairman?

Senator CHAMBLISS. Yes?

Mr. HUTCHINSON. Could I quickly respond on that, as well? I think if there was a 1-year extension, where we would be in a year is that we would be back here reporting that some countries have moved forward quickly in compliance. They will all have a program, but they will not be issuing the biometric passports. We will have just completed the testing phase.

Probably the greatest concern would be that some countries might move forward because of that deadline with technology that has not been sufficiently tested, that would not be in line with the international protocols, that would wind up having something out of sync which would have to be redone and would also put a question mark for our ports of entry, that we might have to develop readers for someone that developed their biometric passports early without sufficient testing and there is a potential for some waste of money in that process, in getting it wrong.

Senator CHAMBLISS. Thank you. Senator Sessions?

Senator SESSIONS. Thank you, Senator Chambliss.

I am concerned about the ability to access the databases, particularly with regard to the visa waiver countries and ICAO, the International Civil Aeronautics Organization's regulations about their adoption of a facial standard. First, let me ask you, Secretary Harty, ICAO is basically a private organization of people involved in aviation that we have—

Ms. HARTY. It is an international organization, sir, and while there may be some private representatives there, every government sends a—every member sends an official government—

Senator SESSIONS. And we pressured them, as I understand it, to come forward with a biometric and they said, okay, facial. But the problem is, facial is not scientifically achievable at this moment and facial is unconnected to this tremendous worldwide databank we have of fingerprints. So we have created a facial identifier that is valid for the purpose of determining whether or not the entering person is the same person holding the passport, but we haven't dealt with any ability to identify those who have records internationally or in the United States of criminal activities.

This is a huge expense. If everybody in the world is going to rush off into this facial idea that may not prove to be practical, it may not prove to be scientifically achievable. As a matter of fact, one major CEO that was in my office and somehow we talked about this subject and he said to me, we chose not to bid on it because we are not sure, this world-class high-tech company, he said, we are not sure we can achieve it. We don't want to end up having false positives and people complaining at us that your system fails. And so we just didn't even bid.

So I guess, Mr. Hutchinson, on the law enforcement side, can't we go back and challenge and urge ICAO to adopt a fingerprint standard that is already in existence worldwide, that we have the proven technology to make it work, and wouldn't that give us a protection that this facial system would not?

Ms. HARTY. Sir, may I answer it, as well?

Senator SESSIONS. Yes.

Ms. HARTY. Thank you. ICAO took quite a bit of time to come up with the facial recognition standard. It was a difficult bar for them to get over. A number of issues came up. The first of those, or one of many, I should say, was the question of what the biometric would be. Lots of people thought, let us look at fingerprints, let us look at hand geometry, let us look at iris scans.

The reason that they went first with facial recognition was they have—every member country has experience collecting photographs because they do that already for passports. The facial recognition technology, as Under Secretary Hutchinson already mentioned, is, in fact, pretty good on one-to-one, which is matching me with my passport, the traveler with the traveler's document. The traveler, of course, goes through immigration and customs in many places, border control, before they leave their own country, entry controls in another country. At each of those border points, there is, of course, access to Interpol information, another layer of that onion, if you will.

But ICAO was also concerned that some countries might want to do more and so they have also acknowledged that other countries might want to collect fingerprints, other countries might want to engage in further studying of iris scans. With respect to fingerprints—

Senator SESSIONS. My time is about up—

Ms. HARTY. I am sorry.

Senator SESSIONS. Let me ask this. I understand ICAO took this option, but it is a no-deal option.

Ms. HARTY. Well—

Senator SESSIONS. You are not going to really help us identify whether or not the person coming in that airport is a fugitive from the United States that fled the country or was deported after having been convicted of a felony. It won't pick that up because our database is not facial. Our database is fingerprint. As the former prosecutor knows, every policeman in America can access anybody and put their fingerprints in a system and on a short notice determine whether or not a warrant is out for his arrest. You can't do that with a face.

And these countries, it seems to me, have an interest, Mr. Secretary. They don't want criminals coming into their country. They don't want fugitives fleeing their country. Aren't we making a big mistake not to push real hard right now to just make this a fingerprint standard?

Mr. HUTCHINSON. Senator, we agree that, first of all, fingerprints should be a significant part of the international criteria for security. We have implemented finger scans through U.S. VISIT. So we have that protection in the United States. But it would also be helpful, as other countries issue passports and travel documents, that they put facial recognition in there, but also another biometric of finger scans or iris scans. Finger scans, obviously, because you have got databases of that collected of criminals around the world.

ICAO did allow that as a secondary. We would like to move the international community to make that mandatory, as well, in the future. Obviously, we don't have a consensus in the international

community to do that at this time, but there certainly would be the law enforcement benefit to do that.

Senator SESSIONS. The FBI Director, Mr. Mueller, said there has got to be interoperability and expansion of the system ourselves, working with the Department of Homeland Security, to be on the cutting edge of the use of fingerprints in all of its manifestations. I asked him about that—that is in response to my question—and he was firm that fingerprints had to be the critical part of the system, in his view.

Mr. HUTCHINSON. We are in agreement on that. The chip standard that is set by ICAO has a sufficient capability to add additional biometrics as those standards are more refined. So, I mean, first of all, Congress set ICAO as the standard to follow.

Senator SESSIONS. That was a Congressional act?

Mr. HUTCHINSON. Yes, that was a Congressional act, to tie this to ICAO.

Ms. HARTY. Yes.

Mr. HUTCHINSON. And so ICAO—

Senator SESSIONS. I am not surprised.

[Laughter.]

Mr. HUTCHINSON. —couldn't do it unilaterally. We have got to do it together.

Senator SESSIONS. Maybe we need to undo that. I mean, it is great to get their opinions and their feedback, but ultimately, it is our borders that we are monitoring.

Thank you, Mr. Chairman. I went over.

Senator CHAMBLISS. Let me just, before we leave that and go to Senator Kyl, U.S. VISIT does require fingerprinting, correct?

Mr. HUTCHINSON. Absolutely.

Senator CHAMBLISS. And in that particular instance, we use those fingerprints to track potential criminals or somebody who has a criminal record and may be trying to get back in here. How does that correlate to the use of the visa waiver program?

Mr. HUTCHINSON. Under U.S. VISIT, right now, all visa travelers, as they come into our ports of entry, our airports, will give their travel document. We will also check their biometric, their two finger scans to make sure it is the same person that the State Department, the consular office has issued the visa to, because they took the same biometric and we have it online transferred to our port of entry. So we have got a one-to-one check. In addition, we will check it against the databases for criminals, visa overstays, immigration violators, and terrorists.

When we add the visa waiver countries on September 30, that same security fix will be in there. The only difference is that we do not have their identity frozen, or their identity verified by the issuance of visas at the consular offices. We check it and it is enrolled the first time and it is frozen whenever they come into our port of entry.

So we use the fingerprints very effectively in U.S. VISIT. I think the only difference, what we are talking about, is if it was an international standard that if it was a French passport, for example, we would have the identity, the biometric, the fingerprint embedded in that French passport. That way, it is an additional security check that would be in place as they came in. That way, we can check

the fingerprint of the person who is coming into that port of entry against the one who the passport was issued to, and that is a huge security benefit.

So we have built the first layer. There are probably additional layers we can build in the future.

Senator CHAMBLISS. Senator Kyl?

Senator KYL. Thank you, Mr. Chairman. Let me just pursue this same line of questioning. In the briefing to staff, I was informed the Department of State did not even raise at the ICAO meetings the use of the fingerprint as the biometric identifier. Is that correct?

Ms. HARTY. Over five years ago ICAO, in its New Technologies Working Group (NTWG), began looking at biometrics for use in tying a person irrevocably to their document. The events of September 11, 2001 and the subsequent U.S. legislation for VWP countries to incorporate biometrics into their passports motivated increased activity in developing biometric studies and programs. In June of 2002, the ICAO NTWG endorsed unanimously the use of facial recognition as the globally interoperable biometric for machine-assisted identity confirmation with machine-readable documents. the BTWG also recognized that some ICAO member states might elect to use fingerprint and/or iris recognition as additional biometrics. Fingerprints were not favored as the primary biometric since many believed the technology raised social and privacy concerns. Furthermore, fingerprints are not currently collected as part of the passport application process; to collect fingerprints would require a new enrollment structure that would be expensive and would require in-person enrollment. The NTWG recognized that facial recognition could meet the business needs of most States in terms of verifying that the person carrying the passport is the person to whom the government issued the passport. In reaching these decisions, ICAO observed:

- Photographs of the face do not disclose information that the person does not routinely disclose to the public.
- The photograph is socially and culturally accepted internationally.
- The public is aware of its use for identity verification purposes.
- It is non-intrusive.
- Many member States have a legacy database of facial images captured as part of the digitized production of passport photos, which can be encoded into facial templates and used for identity comparison.

In May 2003 ICAO adopted a global, harmonized blueprint for the integration of facial recognition into passports. In May 2004, ICAO adopted refined standards for incorporating facial images into the chips to be included into the documents.

Section 303 of the Enhanced Border Security Act of 2002 which required VWP countries to produce biometric passports relied on the ICAO standard; VWP countries have already invested considerable time and money in biometric passport programs based on the U.S. legal requirement and ongoing ICAO discussions of the issue. Inclusion of fingerprinting as a mandatory ICAO standard at this point would further delay the introduction of biometric passports

and would also lead to a reciprocal requirement for U.S. citizens to provide fingerprints.

Senator KYL. All right, because clearly, it is something that we would have wanted to pursue, it seems to me, for the reason that the Secretary just pointed out. What percentage, roughly, of the people coming into the United States today and the people leaving today are covered by U.S. VISIT?

Mr. HUTCHINSON. Well, to give you an idea of the numbers, we have, I think it is 23 million visa travelers. We are adding 13 million visa waiver travelers just to our airports and seaports. That is 36 million. We have a couple hundred million that come in each year. Those are through our land ports of entry, which we will be having U.S. VISIT apply to by the end of this year at the 50 busiest ports. So we are gradually building on the land side. But right now, it is probably, all total, up to 25 percent would be my rough estimate. I would be glad to get you more specifics.

Senator KYL. I realize it is a very rough estimate. The point I was trying to make is just in a notional way that maybe a quarter of the people are being checked today and it is going to take quite a long time for it to expand to the full number of people that we would like to have the U.S. VISIT program apply to, both entry and then exit.

Any estimate with respect to how we are coming along on that, assuming you get the appropriations you need from Congress, how long it will take to get to 100 percent coverage?

Mr. HUTCHINSON. Well, our deadline is the end of this year, 50 land ports of entry, and then a comprehensive system by the end of 2005. That is going to be a very difficult, challenging deadline to meet. We are committed to doing that. And that will not give us necessarily a biometric check of every person who comes across the land borders. You can imagine the complexities there. But it will give us, hopefully, the capability of checking in, checking out every international visitor, which is a huge step forward in terms of determining visa overstays.

Senator KYL. The key point that I would like to make to both of you is that there are questions about whether or not we have tried hard enough to get our friends in other countries to meet the compliance date. We understand that it is impossible to meet the date. We need more time. You have in place a series of checks, milestones to meet. I think it is critical that you supply that information to us on an ongoing basis so we know how it is going. Some members want to suspend the visa waiver for any country until it actually complies. I mean, that is the kind of thing you are facing here. So I think you have got to figure out a way to keep us informed of how well you are doing with both the carrot and the stick.

I also want to ask you a question with regard to one country of particular concern. Ms. Harty, you were kind enough to respond yesterday to a letter that I had sent on May 5 regarding statistics for those who want to visit from Saudi Arabia, the statistics on the applications there, and it appears to me, based upon these statistics, that there is about an 85 percent visa grant rate at the present time. If that is incorrect, tell me.

I don't know how that compares to the rates in some other countries and I would like to ask you to give me some information in that regard. My understanding is that refusal rates, for example, for Egypt and Yemen before September 11 were about 40 percent, and if we are granting 85 percent of Saudi nationals at this point, that seems to me to be a very interesting statistic. Could you shed some light on that for me?

Ms. HARTY. Sure. I would be happy to, sir. If you look at fiscal year 2001 of those statistics I gave you, the number of non-immigrant visas issued in fiscal year 2001, we issued 45,411 visas to Saudi nationals. In fiscal year 2003, which is the most recent, obviously, complete year that I have, we issued 9,862. You have seen such a precipitous drop-off in the number of Saudi travelers to this country. What you have seen, I think, in the largest measure is people who used to come here, as I have heard all over the country, sir, people who used to come here as students, people who used to come here for medical treatment, people who used to come for tourism.

I will have to check it and dig down a little bit, sir, but my hunch here is that that less than 10,000 that we issued in fiscal year 2003 represents people who are coming here in official capacities. We have, until fairly recently, done quite a bit of training of Saudi military officials in this country—

Senator KYL. Excuse me for interrupting, but because of the time, really, my question, if I could, Mr. Chairman, if you would indulge me, with regard to these statistics, first of all, you have to add the two columns, issued and refusals overcome in order to get the total number granted, right?

Ms. HARTY. Yes. I just couldn't do the math quickly enough.

Senator KYL. Right. And secondly, what I am focusing on is not how many Saudis want to come here and are granted a visa but how many refusals there are.

Ms. HARTY. Right. No, no, I understand that. What I was getting at, the last point I would have made there, sir, is that these represent, I believe in large measure, folks that we had a U.S. Government interest in having in the country, the people we were bringing here to train and people on sort of official sponsorship of one kind or another. An awful lot of personal preference travel from Saudi Arabia is just gone. We are just not seeing it. But I can dig down for you, sir, and we will get you a little more.

Senator KYL. Excuse me, Mr. Chairman. If I have additional questions—and I appreciate the information—

Ms. HARTY. Of course.

Senator KYL. I will give those to you in writing and you can respond. Thank you very much.

Ms. HARTY. Okay. Thank you, sir.

Senator CHAMBLISS. Senator Feinstein?

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

Senator FEINSTEIN. Thank you very much, and I am sorry I couldn't be here. I had an amendment on the floor, Mr. Chairman, but I want to welcome Mr. Hutchinson and Ms. Harty to the Committee and use my time really to indicate to you, because you have

been listening in the past and I very much appreciate that, I think the visa waiver program is the soft underbelly of our Nation's guard against terrorism efforts.

We know that slightly below 200 people who are criminals have used the program to come into the country. We know that among them were a number of terrorists, from Ramzi Yousef to Mr. Moussaoui. And we know that about 13 million people from 27 countries come in.

As a member of the Intelligence Committee, I happened 1 day to run across a classified FBI memo which discussed stolen travel documents from a visa waiver country, and I believe you know to what I am referring. Well, then right after that, shortly thereafter, I read the Office of Inspector General, the OIG report on the visa waiver program, which pointed out its weak management, its sloppy organization, really the inability to even know whether people leave the country.

As I began to talk about it, of course, I began to get calls. Oh, you can't do anything about it, you know. This will hurt our business. At the same time, those things that this Committee talked about, and I have been on the Immigration Subcommittee and the Judiciary Committee for 12 years, was the biometric passport, and I remember the discussions. We asked the Department, how long will it take, and they gave us a time and then we even built into that an extra period of time.

Well, that time went by. We have extended it 1 year. Now we have another request to extend it another 2 years. I am really worried because of the specific nature and numbers of stolen travel documents, and particularly when they are counterfeit-proof, what is going to happen. So I am concerned about continuing a program where we can't really, except by manual means, even intercept those fraudulent passports, according to the OIG report, and then very often when we do and it is a counterfeit passport, it is given back to the individual and the reason is so they can get back in their country.

Well, it seems to me if you are using a stolen passport, there ought to be a penalty for that. I, for one, am not concerned about facilitating the user back to his or her country. It seems to me that person ought to be taken into custody, and if the laws need to change to do that, we ought to do it. But as long as we have a laissez-faire system with respect to the use of stolen passports, and I don't believe for a minute that a user of a stolen passport doesn't know that it is stolen.

So I have been thinking, now should I stir the pot by introducing legislation to put a moratorium on the program until the management reforms called for by the OIG are in effect, until we know we have got the passport stipulations of the legislation in place, and until we can say to the people of America, we can account for everybody that comes into this country and we know they leave and we know they are legal and bona fide. If you would like to answer that, I would be happy to hear the answer to it.

Mr. HUTCHINSON. Senator, I would be grateful for the opportunity. We share your concerns on security. Our response has been a very aggressive and, hopefully, thorough approach to enhancing the security in terms of our visa waiver country travelers, both by

enrolling in U.S. VISIT effective September 30, and you did point up very appropriately the comments of the Inspector General. We take that report very seriously. I signed off on a response to each of the recommendations on May 27.

Many of the criticisms that were leveled have been addressed. For example, the oversight, the visa program office has been established within my directorate. We are aggressively pursuing the site visits with the Department of State. We have completed 12 site visits of the visa waiver countries. Two are in progress. The rest are scheduled and will be completed by July 15. We are on target to complete the assessment, which will be the first assessment by the Department, by September 30.

In terms of the passports, again, you are absolutely correct. That is a serious concern. That is one of the requirements to be a visa waiver country, they have good reporting capability for stolen passports. We have that information. When it is provided to us, it is given to our inspectors at the ports of entry. We certainly, if somebody travels here, I think there is a little bit of a misperception that we actually physically give it back to the traveler to return home. It is delivered separately to the law enforcement officials on the other end, is my understanding of it, and we certainly should not be giving it back to them.

Senator FEINSTEIN. I think you ought to check that out, because Secretary Ridge was before us and he said that was the reason that the passports were given back to the individual.

Also, just in this report, it indicates that even when the stolen serial numbers are known, unless it is manually picked up—and this report is just a month old—unless it is manually picked up, it goes by the by.

Mr. HUTCHINSON. Correct, Senator. That needs to be improved. We are working on a data sharing arrangement with Interpol and our European colleagues. So there will be a database that will electronically transfer the stolen passport information. We do have, as they reported, it is put into our system. We do need to enhance that. That is one of the arrangements that we hope to have with our European colleagues in reference to Interpol.

So again, I would simply agree with many of the security concerns that you expressed. I think you have to answer a fundamental question: Should you cancel a program or whether you should enhance the security to make it effective. Until Congress directs otherwise, we are working very hard to make it more secure.

Senator FEINSTEIN. What should we do with someone who uses a forged or stolen passport?

Mr. HUTCHINSON. I would—well, you have got a couple questions there. By and large, I think it should be presented for prosecution to the U.S. Attorney, and you certainly know, Senator, that many of the U.S. Attorneys have guidelines that they are not going to prosecute that case. And so then we are caught with the option of letting him go free in the United States. We are not going to do that, so we have to return him at that point. So prosecutorial guidelines are an issue. Of course, you have some circumstances that an asylum seeker would have a false passport. That has to be evaluated. So we have to make the—but from a law and order

standpoint, I would love to see them prosecuted whenever they come in with that.

Senator FEINSTEIN. Mr. Chairman, if you would just permit me, most asylum seekers aren't necessarily from visa waiver countries. Visa waiver countries are really our strongest positive relationships. So it is really false use of the visa waiver passport. And when you have many thousand of them out on the market, you can be sure they are being used. Otherwise, why steal them if you are not going to sell them? Why steal them in lots of thousands, including other travel documents which then bolster the passport and make it impossible to pick that person up? That is why it is an insidious situation.

Mr. HUTCHINSON. There is not hardly a greater tool that could be used by the terrorists. If they obtain stolen passports, they can utilize them, but they can also sell them on the market and make money. So they almost get a "two-fer" for stolen passports. That is one of the reasons, of course, the enrollment of the visa waiver country travelers in U.S. VISIT, taking their biometric when they come through, is an added security benefit. And as we were talking with Chairman Chambliss, we certainly hope that, eventually, we can require our visa waiver countries to actually have additional biometrics in their passports other than simply facial identification that would give us even a greater security capability.

Senator FEINSTEIN. Would you support strengthening the law with respect to the use of a passport fraudulently in the visa waiver program?

Mr. HUTCHINSON. Strengthen law on the use of a fraudulent passport?

Senator FEINSTEIN. That is correct.

Mr. HUTCHINSON. Well, I think that we could strengthen law, whether it is visa waiver or otherwise. I certainly believe that we can look at that and should look at ways to discourage and to penalize those that would intentionally use a false passport.

Senator FEINSTEIN. Would you do that and make some recommendations to this Committee?

Mr. HUTCHINSON. I would be happy to look at that and certainly work with the Department of State on that and provide a report to you.

Ms. HARTY. If I could add just one line there, I would not only agree with Under Secretary Hutchinson, but I would like to see the law for the use of a U.S. passport which might be fraudulently obtained or used also strengthened with stronger prosecutorial guidelines. Some see the use of a U.S. passport obtained fraudulently as nothing worse than fishing without a license. That is a serious issue and we would love to see those prosecutorial guidelines strengthened, as well.

Senator FEINSTEIN. Mr. Chairman, it is my view, and I would be interested in what Senator Sessions would think, since we are waiting for Senator Grassley, that if we are going to keep this program going, even in view of this report, and I don't know, despite Mr. Hutchinson's good management, I don't know how effectively you can move in a month to solve a lot of these problems, but if we are going to keep it going and actually extend the deadline, it seems to me there ought to be a very strong penalty to use a fraud-

ulent passport, a fraudulent international driver's license, a fraudulent Geneva Convention travel document, or any other document as part of the visa waiver program. And the individual that does should be picked up coming in, should be put in jail, and should be prosecuted, and we ought to send that message out.

Senator CHAMBLISS. Let me say two things. First of all, before you got here, Secretary Hutchinson addressed the IG report and there have already been some corrections made, actually before, I think, the report came out. I know you and I had some conversations about that and I wanted you to be aware of some of those changes that have been made.

Secondly, I don't think there is any question but that anybody who uses a stolen or fraudulent passport seeking to come into the United States is coming here up to no good. Times have changed. It used to be that we didn't need to be as concerned as we do now. We know that on September 11, we should have been more concerned about that. I think you are absolutely right that it behooves us to consider some strengthening of the criminal action that is available to prosecutors for folks who are caught using false stolen passports, as you say, driver's licenses, Geneva Convention documents, whatever.

I would be very receptive to any recommendations that either State or Homeland Security or the Justice Department has in that respect. I think it ought to come from all three of you.

Senator SESSIONS. Mr. Chairman—

Senator CHAMBLISS. Senator Sessions?

Senator SESSIONS. Following up on Senator Feinstein's suggestion, while we act like United States Attorneys get to set prosecutorial policy, they are appointed by the President of the United States to carry out his policies. Mr. Hutchinson was one. I served one 12 years. If the President says, prosecute document fraud cases, if the Department of Homeland Security goes to the Attorney General and says, we want to see some of these cases prosecuted, they will be prosecuted.

Now, you go to the United States Attorney in Los Angeles and he thinks he is too big to prosecute a little case and he wants to prosecute a $100 million bank fraud. But I think that is the wrong way to think, because if nobody will prosecute these cases, they don't get prosecuted. What are they doing every day?

So I do think that we need some directives from the top. I think the way it should occur is that Secretary Ridge should talk with Attorney General Ashcroft, and Attorney General Ashcroft needs to tell some United States Attorneys to prosecute these cases, and I will tell you what will happen. They will start talking and then you will find out who made these false IDs and one person is making thousands normally. So it is not just one case. It can eliminate whole rings of fraudulent document cases and create an impression around the world that if you get caught in the United States with a false document, you are going to jail. And I think the tide can be turned easier than some people think.

I will just say this. These cases don't go to trial. It is not going to back up the whole court system. Most of them are going to plead guilty, Senator Feinstein. You have got them and the document is false. They obviously are not the same person. They have to plead

guilty. Send them to some time in jail and move them out of the country. But the condition—

Senator FEINSTEIN. Now, it is—

Senator SESSIONS. —should be they should tell where they got that document so we can follow up on it.

Senator CHAMBLISS. I think you are probably right that when they do catch them with them, they just don't let them in the country and they send them back—

Senator FEINSTEIN. Right.

Senator CHAMBLISS. —and you are exactly right. We need to send a strong, clear message. If you try to come in here with a fraudulent, stolen passport, you are going to be prosecuted and you are going to jail. It is simple enough. It is much harder to enforce, though, I expect, Secretary.

Does anyone else have any questions? We have got ten minutes left on a vote.

[No response.]

Senator CHAMBLISS. If not, Secretary Hutchinson, Secretary Harty, thank you very much for being here. We appreciate the work that you folks are doing down there. We know it is difficult and tedious, but there is no more important time in the history of our country for the work that you are now doing and we look forward to continuing to work with you. Thank you very much.

The Subcommittee is adjourned.

[Whereupon, at 12:20 p.m., the Subcommittee was adjourned.]

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

QUESTIONS AND ANSWERS

United States Department of State

Washington, D.C. 20520

July 27, 2004

Dear Mr. Chairman:

Following the June 15, 2004 hearing at which Assistant Secretary Maura Harty testified, additional questions were submitted for the record. Please find enclosed the responses to those questions.

If we can be of further assistance to you, please do not hesitate to contact us.

Sincerely,

Paul V. Kelly

Paul V. Kelly
Assistant Secretary
Legislative Affairs

Enclosure:
As stated.

The Honorable
Orrin G. Hatch, Chairman,
Committee on the Judiciary,
United States Senate.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#1)
Senate Judiciary Committee
June 15, 2004

Question:

In April I asked for a comprehensive outline in the steps that are to be taken to ensure the compliance of Visa Waiver Program countries with an extended deadline. I received a short document put together by the State Department, which outlined some of those steps. The document mentioned that the issue would be raised at the upcoming G-8 Summit in June and that Department Principals would get involved in the discussion at appropriate times. Was the biometric passport deadline discussed at the June 2004 G-8 Summit in Georgia? If so, what was the result? Have State Department principals broached this topic in other discussions with principals of foreign nations?

Answer:

The G-8 agenda included an item on secure and facilitated international travel. Under Secretary for Economic Affairs Al Larson was the primary senior State Department official participating in these discussions in which compliance of VWP countries with an extended deadline was raised. The Under Secretary reported on the U.S. program to produce biometric passports and noted we were encountering the same technological challenges as other countries moving to produce biometric passports. He stressed that now that the ICAO standards were set, we must all move aggressively to begin production.

The G-8 agreed to work with ICAO and others to strengthen international standardized practices for passport issuance, and encourage their adoption and implementation by all governments by the 2005 Summit. They also agreed to accelerate development of international standards for the interoperability of government-issued smart chip passports and other government-issued identity documents and to work for implementation by the 2005 Summit.

Foreign Secretary Straw of Britain and Foreign Minister Downer of Australia have both corresponded with Secretary Powell on the subject of compliance with the VWP deadline. Secretary Straw, in two different letters, indicated the need for an extension to the deadline, as Britain would not be producing biometric passports on a significant scale until early 2006. Foreign Minister Downer indicated that Australia was on pace to be able to produce chip-enabled passports by the 10/26/04 deadline; however, the program was dependent on government funding which would probably not be forthcoming if DHS was unable to install the readers at U.S. Ports of Entry to read the passports.

We have continued discussions on how countries are progressing in producing biometric passports, most recently in the ICAO meetings held in

Montreal in May, with the Five Nations group (UK, US, Canada, New Zealand and Australia) in June, and at a European Union meeting in The Hague the week of June 28th. Several countries (Australia, New Zealand and perhaps others) will be participating in DHS sponsored reader testing in Morgantown, Virginia later this month and in Australia in August. We have also called in representatives from the VWP embassies in Washington to discuss the deadline, once in March and again in June.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#2)
Senate Judiciary Committee
June 15, 2004

Question:

Why did the State Department and other government entities not push to ensure that fingerprint scanning be used as the ICAO biometric standard for passports from Visa Waiver program countries?

Answer:

Over five years ago ICAO, in its New Technologies Working Group (NTWG), began looking at biometrics for use in tying a person irrevocably to their travel document. The events of September 11, 2001 and the subsequent U.S. legislation for VWP countries to incorporate biometrics into their passports motivated increased activity in developing biometric studies and programs. In June of 2002, the ICAO NTWG endorsed unanimously the use of face recognition as the globally interoperable biometrics for machine-assisted identity confirmation with machine-readable documents. The NTWG also recognized that some ICAO member states might elect to use fingerprint and/or iris recognition as additional biometrics. Fingerprints were not favored as the primary biometrics since most viewed the technology in conflict with social and privacy concerns of its citizens.

Furthermore, fingerprints are not currently collected as part of the passport application process; to collect fingerprints, we would require a new enrollment structure that would be expensive and not satisfy the needs of most application and renewal processes since in-person enrollment would be required. The NTWG recognized that facial recognition could meet the business needs of most States in terms of verifying that the person carrying the passport is the person to whom the government issued the passport. In reaching these decisions, ICAO observed:

- Photographs of the face do not disclose information that the person does not routinely disclose to the public.
- The photograph is socially and culturally accepted internationally.
- The public is aware of its use for identity verification purposes.
- It is non-intrusive.
- Many member states have a legacy database of facial images captured as part of the digitized production of passport photos, which can be encoded into facial templates and verified against for identity comparison.

In May 2003 ICAO adopted a global, harmonized blueprint for the integration of facial recognition into passports. In May 2004 ICAO adopted refined standards for incorporating facial images into the chips to be included into the documents.

Section 303 of the Enhanced Border Security Act of 2002 requiring VWP countries to produce biometric passports references the ICAO standard; VWP countries have already invested considerable time and money in biometric passport programs based on the U.S. legal requirement and ongoing ICAO discussions of the issue. Inclusion of fingerprinting as a mandatory ICAO standard would lead to a reciprocal requirement for U.S. citizens.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#3)
Senate Judiciary Committee
June 15, 2004

Question:

What is the State Department's current, official position on the interviewing of visa applicants? Does that practice differ for countries with connections to terrorism?

Answer:

General guidance on interview requirements is contained in 9 FAM 41.102 N2. State Department regulations have always included a general requirement that all aliens applying for a non-immigrant visa be personally interviewed by a consular officer, but provided latitude for consular officers in individual posts to waive the interview requirement in certain cases.

Current Department policy is to interview all applicants for non-immigrant visas unless they are under 16 or over 60 years old, are applying for diplomatic or official visas, are seeking a visa in the same classification from the consular post at his or her usual residence within 12 months of the expiration of a previous visa, or for whom a waiver of personal appearance is warranted in the national interest or because of unusual circumstances, as

determined by the consular officer. The consular officer must document the justification for the waiver of personal appearance in these circumstances.

In addition to the personal appearance requirement outlined in 9 FAM 41.102 Note 2, all persons applying for non-immigrant visas ages 14 - 80 have to appear in person for biometric data collection to take two fingerscans electronically. The only exemptions to this requirement are officials applying for A or G visas and individuals who are seeking urgent medical treatment. Persons who might otherwise have their personal appearance waived by a consular officer, therefore, must nevertheless come to the consulate to have their fingerprints scanned.

Applicants from one of the six countries designated as state sponsors of terrorism require the submission of Security Advisory Opinions (SAO) to the Department of State and must be interviewed (required in 9 FAM 41.102 N2.3). This note is currently being revised, however, to allow waiver of interviews for applicants for category A (government official) and G (international organization official) visas who are from state sponsor of terrorism countries.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#4)
Senate Judiciary Committee
June 15, 2004

Question:

What was the State Department's official position on the interviewing of visa applicants before September 11, 2001?

Answer:

State Department regulations have always included a general requirement that all aliens applying for a non-immigrant visa be personally interviewed by a consular officer, but provided latitude for consular officers in individual posts to waive the interview requirement in certain cases. Consular officers were able to issue visas to certain classes of individuals that were not likely to be refused or found ineligible for a visa without their having to come to the consulate for a personal interview. These exceptions were made on a case-by-case, country-specific basis, after reviewing the past record of similar groups of applicants. However, consular officers have always had the authority to call in such persons for personal interviews when warranted. There were also certain classes of persons, such as applicants previously refused visas, persons resident outside the consular district, persons having CLASS hits, or, persons identified as being high fraud,

refusal or security risks, that could not have the interview requirement waived.

Throughout much of the 1990s, consular workload increased without matching resources in personnel or funding. Maximizing available resources – particularly time and space – to provide an equitable balance among protection of U.S. borders, enforcement of immigration laws, efficiency, and customer service was a driving factor in determining pre-9/11 interview policy. Hence, interview by exception policies were used by some posts to adjudicate cases of low-risk applicants. This left more time to concentrate on more problematic cases. GAO reports issued in 1992 and 1998 recognized this and spoke favorably of efforts to identify applicants who would not require interviews. That said, neither post-specific interview by exception policies nor worldwide personal appearance waiver guidelines guaranteed that particular applicants or groups of applicants would be exempted from interview. Interviews were required for some applicants in interview-waived categories based upon questions that arose from the documents submitted.

The State Department policy on the interviewing of visa applicants before September 11, 2001 is described in the following Foreign Affairs Manual reference, which was in effect at that time:

9 FAM 41.102 N1 Personal Appearance and Interview

Section 222(e) of the Immigration and Nationality Act, as well as §41.101 N3 and §41.102 N2 cover the general requirement that all aliens applying for a nonimmigrant visa appear before, and be interviewed by a consular officer, unless the consular officer waives the personal appearance. The consular officer shall determine, on the basis of the applicant's application and interview:

(1) The applicant's eligibility to receive a visa, and

(2) The proper nonimmigrant classification of the visa applicant.

9 FAM 41.102 N2 Waiver of Personal Appearance

Waiver of the applicant's personal appearance does not relieve the consular officer from responsibility for the final decision. A personal appearance may be waived, at the consular officer's discretion, in the case of a nonimmigrant visa applicant who:

(1) Is under 14 years of age;

(2) Is classifiable under the visa classification symbols A, B, C-1, G, H-1, I or NATO;

(3) Makes application for a diplomatic or official visa;

(4) Is classifiable under the visa classification symbol J-1, and who qualifies as a leader in a field of specialized knowledge or skill. The J-1 visa applicant must also be the recipient of a U.S. Government grant, and his or her spouse and children must qualify as J-2 visa holders;

(5) Is an aircraft crewman classifiable under INA 101(a)(15)(D). The application must be supported by a letter from the employing carrier, certifying that the applicant is, indeed, employed as an aircraft crewman; and

(6) Satisfies the consular officer that a waiver is warranted in the national interest, or because of unusual circumstances, including hardship to the visa applicant.

9 FAM 41.102 N3 Personal Appearance in INA 212(d)(3)(A) Waiver Cases

Ordinarily, a personal appearance should be required of any alien for whom a waiver of visa ineligibility under INA 212(d)(3)(A) is sought. However, if the applicant is otherwise qualified as a nonimmigrant, the officer may waive a personal appearance if:

(1) Sufficient information is available on which to base a request for a waiver of personal appearance; and

(2) No collateral intelligence purpose would be served by the applicant's personal appearance.

9 FAM 41.102 N4 Personal Appearance Required

A personal appearance is required for applicants who:

(1) Do not reside in the consular district where he or she is making application;

(2) Were previously refused visas (unless the refusal was overcome);

(3) Are the subject of a CLASS hit, or require a security advisory opinion or other Department clearance; (exceptions can be made for A and G visas); and

(4) Are identified by post as belonging to a group or sector of its visa clientele representing high fraud risk, high refusal rates, or a security threat. (For example, if post has found first-time students to be a particular problem, their interviews should not be waived.)

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#5)
Senate Judiciary Committee
June 15, 2004

Question:

What changes have been made by the State Department, since 9/11, with respect to training new consular officers? What law-enforcement techniques are now taught to consular officers?

Answer:

Consular training goals are to defend U.S. borders and protect American citizens. These goals are stressed in all consular training classes at the Foreign Service Institute (FSI) at the National Foreign Affairs Training Center (NFATC). We emphasize the notion of "security first." Each year, over 2,000 students receive consular training in 15 different courses.

Our basic consular training, also called "ConGen," consists of 31 days of intensive training in the four topical areas: nonimmigrant visas, immigrant visas, U.S. citizenship and American Citizen Services. In ConGen, students are given classes on numerous more specific topics, including anti-fraud methods and anti-terrorism information. More than 500 new consular officers take ConGen each year. ConGen students get individualized

attention in classes of eight students or less. Classes also cover such topics as internal controls (numerous times), management issues and ethics.

Changes in Consular Training since 9/11/01:

- We have added four security/counter-terrorism sessions to ConGen since 2001. These are monthly sessions attended by every student. Two of those classes deal specifically with counter-terrorism information, one of which is run by CIA/CT staff. The other session is a presentation on the consular officer's role in counter-terrorism, presented by the Secretary's Coordinator for Counter-Terrorism.
- ConGen now also includes a third new session run by Diplomatic Security on visa fraud and malfeasance, which includes a piece on how to protect against visa fraud. The fourth "add-on" session is a lecture on how consular officers should use section 212(a)(3) - the terrorism provision of the Immigration and Nationality Act.
- In 2002, we changed the way we conduct interviewing training, and added four and a half new hours of class-time on the theory and practice of NIV interviews.
- In October 2003, we finished a complete revision of ConGen and introduced a new 31-day curriculum (replacing a 26-day schedule).

We added a two-day segment on analytic interviewing techniques, one day to integrate counter-terrorism sessions which were added in 2002-2003, and two days to add more coverage for existing curriculum areas that deserve more time or emphasis.

- In order to bring expertise on interviewing and deception-detection to our students, we contracted with outside interviewing experts (the Institute of Analytic Interviewing) to develop training specifically designed to improve the interviewing skills of consular officers. We took IAI's training specialists to our Embassies in Cairo and Mexico to see live visa interviews and then brought them to FSI to see and critique our existing interviewing training. As a result, we collaborated with IAI to develop and then we introduced a stand-alone, two-day module on analytic interviewing into the new curriculum in November 2003.
- In January 2004, we developed a one-day version of the interviewing training, which can be used outside of ConGen. This module was first introduced to 30 officers at a consular conference in Warsaw in early 2004 and is now part of the Advanced Namechecking course and the mid-level training courses at FSI. In FY 2005 this training will be made available overseas.

- One of our most important courses is the Advanced Consular Name-checking Course - PC 126. This 4-day course was added to our curriculum in March 2002. It is designed to give students an advanced understanding of name-checking theory and practice. Among other topics, students learn about the language algorithms used in the Consular Lookout and Support System (CLASS). To date, we have trained 300 officers in this important course. We plan to train at least 30 additional students in FY 04.
- We lengthened and strengthened the sessions on management issues and added a review of the consular systems applications at the end of the course.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#6)
Senate Judiciary Committee
June 15, 2004

Question:

What has the State Department done to increase the average tenure/experience of consular officers and their direct supervisors? What is the State Department doing to encourage more senior Foreign Service Officers to serve as consular officers in places like Saudi Arabia?

Answer:

The State Department, after many years of hiring to less than attrition, has begun to hire much larger numbers of Foreign Service officers in all areas of expertise, including consular officers. This program, called the Diplomatic Readiness Initiative (DRI), will provide the Department over time with the full complement of officers needed to carry out the important work of the Foreign Service, including consular work. The Bureau of Consular Affairs has added to these numbers of relatively newly hired officers by funding additional Foreign Service officer positions in various posts where more consular manpower was required.

In addition to increased hiring, the DRI allowed an increased emphasis on language skill. Foreign Service candidates may receive additional credit for bringing Critical Languages (e.g. Arabic, Farsi, Dari) into the Service; language training for new officers has also been increased, with new officers receiving 34 weeks plus of training in hard languages. We are also developing "beyond 3" language training for officers to take their skills well beyond the basic competency level. We continue to encourage officers to take up these difficult assignments, including assignments in Saudi Arabia, where our posts are now on ordered departure due to increased danger.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#7)
Senate Judiciary Committee
June 15, 2004

Question:

What concrete steps is the State Department taking to ensure that all posts are fully participating in the Visa Viper program to identify potential terrorists who have not necessarily been added to the terrorist watch list?

Answer:

The Department frequently sends cables to the field reminding embassy and consulate staff members of the importance of the Visas Viper program in helping to protect our national security. One recent cable was from Under Secretary for Management Grant Green directly to the attention of all chiefs of mission stressing the importance of the program and the requirement that all posts submit monthly reports, even negative ones. Under Secretary Green reminded the chiefs of mission that the Secretary himself was personally interested in the program and in posts' monthly compliance with reporting requirements. We have also instituted a monthly cable to all posts which lists all the Visas Viper reporting cables that have been received and processed during a given month.

When a post is late in submitting its mandatory monthly Visas Viper report, the Department sends a reminder cable requesting that the report be submitted as soon as possible.

In the first quarter of this year, the Department achieved 100% compliance in monthly reporting from all posts.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#8)
Senate Judiciary Committee
June 15, 2004

Question:

Please provide me with the 2001 to the present, visa-issuance and refusal rates for nationals inside Yemen, Oman, Algeria and Egypt. How do the 2001 to the present visa-issuance and refusal rates for Saudi Arabia nationals compare to the refusal rates for countries such as Egypt, Yemen, Oman or Algeria?

Answer:

The Department generally releases to the public only those refusal statistics published in the annual *Report of the Visa Office* (i.e. worldwide refusal and overcome statistics by total applicants and grounds of ineligibility). We also on occasion release refusal data for specific visa categories on a worldwide basis. We do not usually release refusal data or refusal rates for specific nationalities or posts, since the data are subject to misinterpretation or misrepresentation by the press or public, could result in invidious comparisons between countries, or could encourage visa shopping. Please find below visa issuance statistics in the categories requested.

Nonimmigrant Visa Workload for Nationals of Algeria, Egypt, Oman, and Yemen Applying at Host Country Posts and for Nationals of Saudi Arabia Applying at Host Country and Third Country Posts and Worldwide Fiscal Years 2001 through 2003, and 2004 to Date * (01-OCT-2003 to 30-JUN-2004)

Nationality/Post	FY	Visas Issued
Algerians at Algiers	2001	3,811
	2002	2,521
	2003	2,125
	2004 *	1,804
Egyptians at Cairo	2001	43,470
	2002	18,077
	2003	13,715
	2004 *	11,431
Omanis at Muscat	2001	2,699
	2002	1,439
	2003	965
	2004*	1,046
Yemenis at Sanaa	2001	1,473
	2002	775
	2003	961
	2004*	662
Saudis at Jeddah	2001	16,483
	2002	4,961
	2003	3,698
	2004*	2,703
Saudis at Riyadh	2001	28,493
	2002	7,792
	2003	6,090
	2004*	5,147
Saudis at Jeddah and Riyadh Combined	2001	44,976
	2002	12,753
	2003	9,788
	2004*	7,850
Saudis at All Posts Except Jeddah and Riyadh	2001	1,660
	2002	1,373
	2003	847

	2004*	1,040
Saudis at All Posts Worldwide (Grand Total)	2001	46,636
	2002	14,126
	2003	10,635
	2004*	8,890

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#9)
Senate Judiciary Committee
June 15, 2004

Question:

The October 21, 2002 GAO report, "Visa Process Should Be Strengthened as an Antiterrorism Tool," gives estimated interview rates by post, and by nationals versus third-country nationals. Please provide those same figures month-by-month, both overall and by post and for Saudi nationals and third-country nationals for 2001 through the present. In other words, please provide the exact number of Saudi nationals or third-country nationals interviewed at either Riyadh or Jeddah for any given month.

Answer:

The Department of State does not maintain exact statistics on interview rates. The rates provided in the GAO report were based on estimates provided by consular managers in Riyadh and Jeddah. Since July 2002, Riyadh and Jeddah have interviewed all applicants between the ages of 12 and 60 with exceptions made only for certain applicants for category A (officials of foreign governments) and G (officials of international organizations) visas.

Embassy Riyadh began collecting biometrics from visa applicants on 11/24/03 and Consulate Jeddah began on 12/8/03. All applicants aged 14 - 79 must make a personal appearance and have fingerscans taken for the visa.

The interviews are still waived for diplomatic and official applicants; however, certain diplomatic applicants are subject to interviews (in particular, A-2 visas applicants for military TDYs).

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#10)
Senate Judiciary Committee
June 15, 2004

Question:

Please provide me with statistics on visa issuances and refusals for Saudi Arabian nationals versus third-country nationals at the Riyadh post, for the Jeddah post, and for Saudi Arabia as a whole. The final table of statistics for Saudi nationals worldwide, which you provided to me on June 15th, though interesting and helpful, is not sufficient. It combines statistics for Saudi nationals applying in the kingdom and those applying in foreign countries, where they are treated, by definition, as third-country nationals, by those posts. I would like those separated.

Answer:

The Department generally releases to the public only those refusal statistics published in the annual *Report of the Visa Office* (i.e. worldwide refusal and overcome statistics by total applicants and grounds of ineligibility). We also on occasion release refusal data for specific visa categories on a worldwide basis. We do not usually release refusal data or refusal rates for specific nationalities or posts, since the data are subject to misinterpretation or misrepresentation by the press or public, could result in invidious comparisons between countries, or could encourage visa shopping. Please find below visa issuance statistics in the categories requested.

Nonimmigrant Visa Workload
For Saudi Nationals and Third Country Nationals
At Consular Posts in Jeddah and Riyadh
Fiscal Years 2001 through 2003, and 2004 to date *
(01-OCT-2003 to 30-JUN-2004)

Nationality/Post	FY	Visas Issued
Saudis at Jeddah	2001	16,483
	2002	4,961
	2003	3,698
	2004*	2,703
Third Country Nationals At Jeddah	2001	8,104
	2002	3,002
	2003	2,498
	2004*	1,275
All Nationalities at Jeddah (Grand Total)	2001	24,587
	2002	7,963
	2003	6,196
	2004*	3,978
Saudis at Riyadh	2001	28,493
	2002	7,792
	2003	6,090
	2004*	5,147
Third Country Nationals at Riyadh	2001	16,917
	2002	5,715
	2003	3,772
	2004*	2,808
All Nationalities at Riyadh (Grand Total)	2001	45,410
	2002	13,507
	2003	9,862
	2004*	7,955
Saudis at Jeddah and Riyadh Combined	2001	44,976
	2002	12,753
	2003	9,788
	2004*	7,850
Third Country Nationals at Jeddah And Riyadh Combined	2001	25,021
	2002	8,717
	2003	6,270
	2004*	4,083
All Nationalities at Jeddah and Riyadh Combined (Grand Total)	2001	69,997
	2002	21,470
	2003	16,058
	2004*	11,933

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#11)
Senate Judiciary Committee
June 15, 2004

Question:

Please provide me with the "Consular Package" for Saudi Arabia (both Riyadh and Jeddah) for each year from 2001 through 2003.

Answer:

The Consular Packages for Jeddah and Riyadh for FY 2001-2003 are being forwarded separately under cover of a letter.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator Jon Kyl (#12)
Senate Judiciary Committee
June 15, 2004

Question:

Please provide me with a copy of the visa application in which Kalid Sheik Mohammed was approved for a visa to enter the U.S. in 1996 through the Visa Express program. What type of consular affairs interview process did Kalid Sheik Mohammed undergo before being issued a visa?

Answer:

Khalid Sheikh Mohammed, a Pakistani national, received a U.S. visa on July 23, 2001 using a genuine but fraudulently obtained Saudi passport under the name of Abdulrahman al Ghamdi. This application is attached. The Visa Express program had become operational in May 2001, but it is not possible to establish if he received his application directly through this program.

The Combined Consular Database does not list an application for "Kalid Sheik Mohammed" in 1996. At that time State Department policy limited retention of issued visa files to one year.

Questions for the Record Submitted to
Assistant Secretary Maura Harty by
Senator John Sununu (#1)
Senate Judiciary Committee
June 15, 2004

Question:

Technology is presently available to compare the passport holder data and photo typefaces and security features in verified passports. I understand that several countries, including Australia, are using such technology to help authenticate passports from many nations. I also understand that the State Department and the Department of Homeland Security ran a series of tests in Nigeria with this process. Do you believe adding such technology to both the biometric-based entry procedures and to the visa-required entry procedures would be a significant additional safeguard to ensure passports have not been altered or otherwise defrauded?

Answer:

The International Civil Aviation Organization (ICAO) has adopted facial recognition as the primary biometric to be included in Passports. ICAO, which is the recognized body for setting international passport standards, has published a standard that calls for including the passport holder's image stored in a contactless chip affixed into the passport. The standard also calls for each government to sign the passport with a digital signature, a very powerful security feature.

Several ICAO member countries, notably Australia, Germany, Canada, Great Britain and the United States, have been conducting applied research and development into facial recognition to demonstrate its

feasibility for improved border control. Australia is testing facial recognition in Sidney through its "Smart Gate" program, currently limited to airline crews. Smart Gate requires each participant to enroll in the program by providing biographic data as well as several facial images. The Sidney airport is equipped with a kiosk that reads the passport and compares the participant's image to that stored from the enrollment. A facial recognition match opens the gate and allows the participant to enter the country without seeing an inspector, while a no match directs the participant to an inspector. Preliminary results have been promising, and Australia is considering expanding the pilot.

The State Department, Bureau of Consular Affairs (CA) has been conducting a facial recognition test with 14 posts, including Lagos, Nigeria. This pilot is directed at detecting potential fraudulent visa applicants who apply under different identities. In this pilot all visa applicants from these 14 posts are compared via facial recognition to photographs of applicants from 100 posts to determine if the applicant had ever applied under a different name. Under this program several hundred fraudulent applicants have been identified, with the majority coming from Nigeria. CA is looking into expanding this pilot.

CA does believe that facial recognition offers great promise for border security. Tests have shown that in the one-to-one comparison, such as the Australian Smart Gate, the facial accuracy is very good and offers great promise for increasing border control security at the airports and land border crossings. Working with DHS, we are planning a pilot test using facial recognition at U.S. airports for passport control. The technical accuracy of facial recognition in the one-to-many scenario, such as our Nigerian test, is not quite as accurate but the technology is rapidly emerging. We have been successful in identifying several hundred fraudulent applicants that we otherwise would not have identified, so we are currently getting positive results which should improve as the technology develops. CA will continue to work both individually and cooperatively with ICAO participants to incorporate facial recognition technology into the border control process.

Written Questions Submitted by Senator Jon Kyl
Hearing Before the Senate Judiciary Committee
June 15, 2004

"Biometric Passports"

Questions for Asa Hutchinson Under Secretary for the Border and Transportation Security Directorate:[1]

1. What role is DHS playing in visa processing? Specifically, what role is it playing in changing and issuing regulations to reform longstanding visa issuance policies and practices, to focus more on security?

Answer:

- Subject to certain exceptions, the Homeland Security Act and the DHS-DOS MOU give the Department of Homeland Security (DHS) the lead responsibility to establish visa policy and final authority over visa guidance concerning: alien admissibility, classification, and documentation; place of visa application; personal appearance/interviews; visa validity periods; and the Visa Waiver Program. DOS has the lead on foreign policy issues and manages the overall visa process, with 211 visa processing posts overseas and two domestic centers to support immigrant visa operations.

- The last three years have been a time of unprecedented change in visa and border management practices. Changes in visa processing implemented after September 11, 2001 include an aggressive effort to improve security, including the requirement of personal interviews, background checks including limited criminal checks, the deployment of visa security officers in some posts, and improvements to the quality of terrorist watchlists. DHS will continue to provide the security perspective on visa policy as we work with DOS on expanding database connections and interoperability of systems.

2. I am aware that you and Secretary Ridge have both questioned the accuracy of the findings in the April 2004 DHS Office of Inspector General Report entitled, "An Evaluation of the Security Implications of the Visa Waiver Program." The Inspector General found mismanagement and a lack of security measures within the Visa Waiver Program, and made recommendations to help make the program more secure. I am aware that at least one of the recommendations, that all Visa Waiver Program participants be subject to U.S.-Visit requirements, was instituted before the report was released, However, I would like to know the accuracy of the remaining findings and the status of implementation of the remaining recommendations.

    a. Which of the report's findings were accurate?

[1] Unless otherwise noted, the following answers are current as of the date of the hearing.

Answer: The report was generally accurate when it described the program, its history, and related legislation. However, the section of the report which addressed the status of the statutory designated country reviews was outdated at the time of the report. This was discussed with the IG's office before the report was published. Before the report was issued, the Border and Transportation Security Directorate (BTS) had already taken responsibility for the Visa Waiver Program (VWP) country review process and reconvened the VWP Interagency Working Group (IWG) originally convened by the Department of Justice's Executive Office of National Security (EONS) prior to the creation of the Department of Homeland Security (DHS) and the transfer of responsibility for the program to the Secretary of Homeland Security. The IWG held its first meeting in early March specifically to develop the plan for the VWP country assessments. In addition, the report recommended that DHS expand US-VISIT to include VWP travelers. DHS had already announced its decision to do so prior to the report's issuance.

b. On how many, and on which, of the report's recommendations has DHS taken action?

Answer: BTS had already taken action on several of the recommendations independent of the report and prior to its issuance. These actions included: assuming responsibility for the VWP and the statutory country reviews, reconvening the interagency working group to conduct the reviews, taking steps to expand US-VISIT to include VWP applicants, as well as including a review of Belgium in the FY 2004 review cycle. BTS has begun action on all of the other recommendations and in the IG's June 23, 2004 reply to BTS' response closed two of the recommendations.

c. What type of action has DHS taken to implement those recommendations? Concerning the recommendations on which DHS has not taken action, which of those does DHS plan address in the future?

Answer: On July 1, 2004, the BTS Under Secretary designated an acting Visa Waiver Program manager with clearly defined responsibilities and authorities. The acting program manager is currently coordinating with DHS components to identify liaisons to ensure the implementation of VWP requirements. The BTS Office of International Enforcement's Visa Waiver Program (VWP) Oversight Unit participates in the US-VISIT Congressional Report Working Group that is developing a plan to ensure the accurate and timely submission of required VWP annual reports on overstay estimates, including the VWP annual reports. This Working Group consists of representatives of all appropriate DHS organizational elements. US-VISIT has responsibility for tracking entries, exits and overstays, and is developing this capability in incremental stages. Over the next several years, US-VISIT will deploy the infrastructure and functionality to enable increasingly accurate and complete overstay reporting. The Working Group is examining the reporting requirements, current US-VISIT capabilities for the initial report to Congress and recommendations for improvements to the initial and subsequent annual reports.

Formal responsibility for conducting the required country reviews has been assigned to the VWP Oversight Unit in the BTS Office of International Enforcement (OIE). By April 2005 the Oversight Unit will develop standard operating procedures for conducting future country reviews and will review, and as appropriate, finalize, modify or revise, the current draft interagency protocol (developed for and used in the prior country reviews and modified for this cycle of country review) after the completion of the current country review cycle. The current (2004) country review process has been managed by the BTS Office of Policy and this responsibility, as well as responsibility for the associated report to Congress, will transition to the VWP Oversight Unit upon completion of the current country review cycle. DHS is working closely with the Department of State in this process. We anticipate the current country review will be completed in early 2005.

CBP will develop an automated mechanism to query the appropriate databases to determine if newly reported lost and stolen passport data has already been used to effect entry into the United States and, if so, will contact the U.S. Immigration and Customs Enforcement liaison officer for investigation. For those passports from countries that do not print serial numbers into passports prior to personalization, CBP will train inspectors on the techniques to identify them as malafide documents. CBP/NTC will also track 'hits' on reported lost and stolen passports to ensure that ports of entry have all relevant information to determine if the document is being used by other than the true bearer. ICE is coordinating with CBP to receive information on individuals present in the United States who entered on a stolen passport and will attempt to locate and remove such persons.

In addition, as part of its oversight responsibilities, the VWP Oversight Unit will work with all appropriate components to review in 2005 a wide range procedures and activities relating to the collection and dissemination of lost and stolen passports.

By January 2005, CBP will establish the Fraudulent Document Analysis Unit (FDAU) to receive, conduct analysis and disseminate information and alerts on foreign passports intercepted at U.S. ports of entry, preclearance operations and Immigration Advisory Program locations. CBP's unit works closely with the Forensic Document Lab. No fraudulent documents will be returned to the traveler. The current review procedures already contain a provision for the review of document manufacturing and issuing security practices. This review is, and will continue to be, in any interagency protocol and will remain an important part of the country site visit.

d. Did BTS ever issue a written response to the OIG report? If not, why not? If so, please provide me with a copy.

Answer: BTS responded in depth to the OIG report and the IG has acknowledged BTS' May 27,2004 in a memo dated June 23, 2004. The response is attached.

Senator Patrick Leahy
Biometric Passports
June 15, 2004
Written Questions for Undersecretary Asa Hutchinson:

1. On June 14, 2004, you joined Attorney General Ashcroft in a press conference announcing the indictment of Nuradin M. Abdi. On its face, the indictment focuses on events that happened long before June 2004 and before Abdi's actual arrest in November 2003. According to the indictment, Abdi is a native of Somalia, and the indictment contains charges that Abdi had lied on travel documents as early as March 2000. Despite this fact, and despite evidence that Abdi was associated with convicted terrorist Iyman Faris for the purpose of using a bomb at a mall in Ohio, the government sought Abdi's deportation in January 2004. As a result, the court ordered his deportation on March 11, 2004 to take place ninety days later on June 11, 2004,

   Then, in what appears to be an abrupt about-face, the grand jury indicted Abdi the day before his scheduled deportation. Up through the unsealing of the indictment, it certainly appeared as if the government intended to release Abdi to Somalia despite the serious allegations against him – giving this matter striking parallels to the reported release of suspected terrorist Nabil al-Marabh to Syria.

   (A) Why did the government initially seek Abdi's deportation rather than indicting him based on events that the government knew about at the time of Abdi's arrest and deportation hearing? If Abdi targeted America, to quote the Attorney General, "for death and destruction by an al Qaeda cell", why would the government ever press for his deportation in lieu of prosecution?

   Answer: Nuradin Mahamoud ABDI is a native and citizen of Somalia who was found to have committed numerous acts of immigration fraud and determined to be a threat to the security of the United States. ABDI first came to the attention of the Federal Bureau of Investigation (FBI) due to his association with and statements made to a self-proclaimed member of Al Qaeda. The statements included an alleged plot involving an attack on an unnamed shopping mall. Upon the eve of the busiest shopping day of the year, the FBI requested that ICE arrest ABDI. On the morning of November 28, 2003, ABDI was promptly arrested by ICE agents assigned to the Joint Terrorism Task Force. ICE attorneys litigated a removal proceeding against ABDI and secured a final order of removal to Somalia on March 9, 2004. The Immigration Judge ordered ABDI to be detained without bond for the duration of the proceeding due to national security concerns.

   At the time of the Immigration Judge's issuance of the removal order, ICE was working closely with the Department of Justice in the Joint Terrorism Task Force investigation to ensure preparation of its criminal case and understood that ABDI would be indicted and thereupon transferred from ICE to Bureau of Prisons'

custody at the appropriate time. ABDI was promptly transferred to Bureau of Prisons' custody following his indictment.

We would also refer the first part of the question to DOJ as they make the determination to criminally prosecute and individual.

(B) Will you provide me with periodic updates on the status of this case and advise me on the details of any resolution?

Answer: ICE can provide updates on the completed removal proceeding. However, ICE would recommend that the Department of Justice provide updates concerning the status of any criminal proceedings.

2. It is my understanding that the chip embedded in the passport will include an encrypted version of complete biometric images rather than encrypted data based on features or "hashing" algorithms of the biometric,

a. Should the images in the system be inappropriately used or hacked — for instance by an insider or contractor — these entire images could become compromised, possibly risking future uses of biometrics as an authentication technology, particularly in contexts that do not allow for additional security checks to detect fraudulent presentation and use of fingerprint images *e.g.,* at-home fingerprint readers that authenticate users for purposes like lap-top and online account access. Was this possibility considered when the decision was made to include complete images rather than features or algorithmic references, and if so, how was this issue resolved?

Answer: The new E-Passports will contain a contactless chip that will hold only the biographic information currently printed in the passport and a digitized "biometric" photograph. The International Civil Aviation Organization (ICAO) has chosen facial recognition as the globally interoperable biometric for inclusion in e-passports. Issuing nations may, at their discretion, include fingerscan and/or iris scan data. In the interest of interoperability, ICAO chose storing images, rather than templates. Templates are extracted information from the image that is used by biometric processing algorithms. The format and content of templates is generally proprietary. If templates were to be chosen, nations reading the data would have to have each template capability for every issuing nation in order to have full access to the information in a usable form. Recently, there has been some progress in making templates more interoperable, but there have been no conclusive results yet. (US-VISIT is funding work by the National Institute of Standards and Technology to examine this area). The facial image (a digital copy of the photograph on the data page) is stored on the chip in the e-passport. There is a 'digital signature' in the stored image that verifies that the image was written onto the chip by the authorized entity. For nations deciding to store fingerscan and iris scan data, they may choose to store that information with additional levels of

protection, including "active authentication and secure messaging" and/or "basic access control." Encryption of that information is also allowed according to ICAO standards.

The relative risks and advantages of images vs. templates were the subject of technical examination and extensive review by the ICAO, with the national bodies and technical experts agreeing that the best approach was to include images. ICAO stated in its Technical Report, *PKI for Machine Readable Travel Documents (MTRDs)Offering ICC Read-Only Access*: "The digitally stored image of the face is assumed not to be privacy sensitive information. The face of the MRTD holder is also printed in the MRTD and can be obtained freely anyway. The digitally stored image of the finger(s) and/or iris are additional biometric features for which States MAY choose to apply for national use. They are generally considered to be privacy sensitive and therefore need to be protected under the issuing State's responsibility."

b. Where is the decryption key stored for the biometric data, and is the decryption key specific to a single passport or based on a global standard?

Answer: There are several keys associated with the storage of information on the e-passport chips. The digital signature (used to verify the authenticity of the data as originating from the stated source) is the first level. The issuing authority (nation) controls the private key, but registers the public key in the Public Key Directory (PKD) maintained by ICAO. This information may also be shared directly between nations. Country Signing Certificates are not part of the ICAO PKD service, but the PKD shall use the Country Signing Certificate to verify the authenticity and integrity of the Document Signer Certificates received from participating States.

The IC chip contains a Document Security Object that is digitally signed by the issuing State and contains representations of the data in the chip's Logical Data Structure (LDS). An inspection system with access to the PKD, or having read the Document Signer Certificate from the e-passport, will be able to verify the Document Security Object, thus verifying the authenticity of the LDS contents.

Issuing States may employ another set of keys for "active authentication." The chip contains its own Active Authentication Key pair, with the representation of the Public Key stored in the Document Security Object and therefore authenticated by the issuer's digital signature. The corresponding Private Key is stored in the chip's secure memory.

"Basic Access Control" (to be used by some nations) requires chip-individual Document Basic Access Keys which are derived from information from the machine readable zone ("MRZ"). A chip that is protected by the Basic Access

Control mechanism denies access to its contents unless the inspection system can prove that it is authorized to access the chip. The proof is given in a challenge-response protocol based on the MRZ data. This schema is used to establish "secure messaging" for the transmission of information between the chip and the reader, based on verification of the data from the MRZ on the printed page compared to the stored data on the e-passport IC chip.

If a nation so desires, there is an additional set of keys that may be employed for "Extended Access Control." Defining the (chip-individual) Document Extended Access Key set is up to the implementing state.

Senator Chambliss
Submitted on behalf of Senator Sununu
Senate Judiciary Committee Hearing on
Biometric Passports

Follow-up Questions

Question for Asa Hutchinson:

Technology is presently available to compare the passport holder data and photo page with typefaces and security features in verified passports. I understand that several countries, including Australia, are using such technology to help authenticate passports from many nations. I also understand that the State Department and the Department of Homeland Security ran a series of tests in Nigeria with this process. Do you believe adding such technology to both the biometric-based entry procedures and to the visa-required entry procedures would be a significant additional safeguard to ensure passports have not been altered or otherwise defrauded?

Answer: There are several systems on the market that allow the comparison of special security features on passports and other travel documents to an established baseline. US-VISIT will be examining the possible inclusion of these analytical tools in the new passport readers that will be required to access the data contained on the IC chips in e-passports. The accuracy of such units and the effect of processing time in primary inspection will be assessed, as well as the potential for use in secondary inspection.

SUBMISSIONS FOR THE RECORD

Hearing Before the Senate Judiciary Committee
"Biometric Passports"

Written Testimony of Senator Maria Cantwell

June 15, 2004

Thank you very much Mr. Chairman for inviting me to testify.

The need for greater border security became glaringly evident in the Northwest in 1998 when Ahmed Ressam, a terrorist trained at one of Osama bin Laden's training camps in Afghanistan, was arrested shortly after crossing the Canadian border at Port Angeles, Washington. Explosives and other bomb-making materials were found in the trunk of Ressam's car. Ressam's plan was to head to Los Angeles to blow up the Los Angeles Airport. Thanks to the work of Diana Dean, the U.S. Customs Inspector, this terrorist was apprehended. This frightening incident made clear the vulnerabilities we face along the porous northern border, vulnerabilities that became even more concerning after the Sept. 11, 2001, terror attacks.

But the Ressam case raises questions about our international standards. Ressam began his journey on a French visa, leaving Algeria and landing in Versailles. Ressam came into the United States after creating a trail of fraudulent documents on his journey from Algiers to the United States – first obtaining a French passport on the basis of a fake French birth certificate; he then entered Canada under his own name, seeking refugee status. While living in Canada, he used a false baptismal certificate to obtain a Canadian passport under an alias.

An international biometric standard for visas would have identified Ressam the first time he tried to enter France. That identification would have been traceable when he entered the United States and he would have more easily been stopped.

In the Patriot Act, I was able to work with Senators Hatch and Leahy to add provisions in to establish technology standards for the U.S. visa program. Those provisions, section 403(c) of the Patriot Act, called for technology standards to facilitate a comprehensive screening of visa applicants at our overseas consulates; access to the necessary law enforcement, watch-list and intelligence information at our consular offices and at border crossings, and verification of the identity of persons crossing our border as being the same person who obtained the travel documents and that the person is someone we would not want to exclude from entering the United States.

In the Enhanced Border Security and Visa Entry Reform Act of 2002, I worked closely with Senators Kennedy, Feinstein, Brownback and Kyl to include in Section 603 a requirement that the Department of State and the Department of Homeland Security coordinate this same technology into their work with Canada, Mexico and the 27 visa waiver countries. This would implement standards for visa programs that would be compatible with those adopted in the U.S.

More simply said, we must recognize that we need international cooperation, we need the international community to adopt visa technology standards compatible with our own. This would enable us to catch the Ressams of the world sooner.

The problem begins in the United States. The requirements of the visa technology standard, like the passport standards, have not been met. Congress required that visa standards be set by 2003. In a report issued in November of 2002, The National Institute for Standards and Technology, the standards body responsible for certifying the standard, recommended dual-biometric for visas: fingerprints and facial recognition. With the US VISIT Program, the Department of Homeland Security has begun to implement a national biometrics program using dual biometrics. But the biometrics chosen don't allow for searching FBI or Interpol databases. More analysis should be done on the appropriate standards.

The Departments of State and Homeland Security, must make it a priority to establish U.S. standards, and to work with the International Standards setting Organization, the ISO, which is the network of national standards institutes from 148 countries, and the International civil aviation organization, to adopt these standards.

We need to stop terrorists before they are at our borders. In fact, we should be working first and hardest in regard to the seven State Department listed "terrorist states." These are the countries in which we must first implement biometric standards in travel documents and make the screening information available to those issuing those documents. It should be the priority.

The 19 hijackers that perpetrated the attack on the U.S. on September 11, 2001 had submitted 24 visa applications, receiving 22 tourist visas and one student visa. The 19 entered the United States a total of 33 times before flying airplanes into the Twin Towers and the Pentagon. We have got to do a better job at securing our visa process.

I am asking this committee to take a very close look at the progress on the international establishment of both the visa standard and the passport standard – these technical matters are inextricably linked in how we protect our borders. Given the significance of these technology standards, and the delinquency in implementing the requirements of the statute, I ask that this committee be updated by the Administration every six months.

Thank you Mr. Chairman for giving me the opportunity to testify.

Statement by Maura Harty
Assistant Secretary of State for Consular Affairs
Senate Judiciary Committee
June 15, 2004

Thank you for the opportunity to testify today on the Administration's request for a two-year extension of the October 26, 2004 deadline for inclusion of biometric features in passports issued by countries which participate in the Visa Waiver Program (VWP). I also want to report on the Department of State's progress in developing our own biometric passport. The inclusion of biometrics in international travel documents to improve our ability to verify the identities of prospective travelers to our country, especially individuals who might present a security risk, is a critical step in improving border security for America and in protecting travelers. The entire international community will benefit from the security advantages of biometric passports as part of our collective effort to combat terrorism.

Naturally, these are not the only steps we are taking with regard to enhancing the security of our borders. We are working hand in hand with our colleagues in the Department of Homeland Security (DHS) to improve our multi-layered and interlocking system of border security through greater information sharing among agencies and with the VWP governments, through enhanced passenger screening and pre-clearance measures, and with DHS's recent decision to expand the US-VISIT Program to VWP travelers. State and DHS are currently in the middle of the congressionally mandated biennial reviews of the VWP countries, assessing their compliance with the terms of the program and the criteria established by Congress. At all visa-adjudicating posts overseas, consular officers have pushed the very borders of our nation far beyond our physical limits as a nation. And through our Visa Viper committees at every post, we aggressively pursue all leads so that every element of the Embassy in a position to do so – all over the world – contributes critical information to our consular lookout systems.

As you know, the Enhanced Border Security and Visa Entry Reform Act (EBSA) established October 26, 2004, as a deadline by which VWP countries must begin issuing their nationals only passports that incorporate biometric identifiers that comply with the International Civil Aviation Organization (ICAO) standards. In May 2003, ICAO decided to make facial recognition encrypted on contactless chips the globally interoperable, standard passport biometric. Thus, VWP countries had 17 months from that decision date to bring a biometric passport from design to production -- a process that normally takes years. The EBSA does not provide a waiver provision, and few, if any, of the 27 participating VWP countries will be able to meet this legislatively mandated deadline. Although the VWP country governments are committed to deploying biometric passports, they are encountering the same technical and scientific challenges we are in our effort to produce a sound biometric passport.

The challenge given the international community by this congressional mandate is a daunting one. We face complex technological and operational issues, including the

security of the passport data on the contactless chips and the interoperability of readers and biometric passports. Working through these hard issues takes time. In May 2004, ICAO established the technical standards for the interoperability of contactless chips and passport readers at ports of entry and the technical specifications for protecting passport data from unauthorized use. As a result, manufacturers can now begin producing passport readers that will be able to read multiple chips.

Each country must now begin limited production of the contactless chip passport for testing. We do not expect to receive large shipments of 64kb chips for use in the U.S. passport until spring, 2005. Like other governments, we expect deliveries to ramp up during 2005, but we ourselves will only be able to complete our transition to a biometric passport by the end of 2005. All of us are engaged in comprehensive testing of the contactless chips, using different technologies to communicate with the chip reader. This testing is designed to ensure that passports and their chips are compatible with passport issuance and border control systems.

Now that we have the technical standards, all VWP countries can begin full development and deployment of their respective biometric programs. However, given the time it has taken to resolve these complex operational issues, few, if any, will be able to meet the October 26, 2004 deadline. For example, none of the larger countries -- Japan, the United Kingdom, France, Germany, Ireland, Italy or Spain -- will begin issuing passports with standardized biometrics by that deadline. The United Kingdom expects to begin in late 2005, Japan to complete transition to full production by April 2006. Others may not come on-line until well into 2006. This delay is not due to a lack of good will but due to significant scientific and technical challenges that has taken us to the cutting edge of changing technologies.

However, there are a number of significant developments in the coming months that will demonstrate how committed nations are to introducing biometrics into their passports. The most important of these is a global interoperability test scheduled for next March involving the United States, Australia, and other nations that will be producing biometric passports at that time. This test will take place in airports and will involve air crew and regular passengers presenting their biometric passport at ports of entry where they will be read electronically. These tests are intended to identify and resolve any problems that may affect the global interoperability of this next generation of passports. These results will be shared with all countries so that the lessons learned can be applied to their biometric passport projects.

Although the legislative requirements of the EBSA apply only to VWP passports and not the U.S. passport, we recognize that convincing other nations to improve their passport requires U.S. leadership both at the ICAO and by taking such steps with the U.S. passport. Embedding biometrics into U.S. passports, that meet the ICAO biometric standard, to establish a clear link between the person issued the passport and the user is an important step forward in the international effort to strengthen border security. To this end, we are introducing "contactless chips" into U.S. passports, electronic chips on which

we will write the same bearer's biographic information that appears visually on the data page of the passport as well as a digitally imaged photograph of the bearer.

As a point of reference, here is the status of our plans to introduce biometrics into U.S. passports. Working in conjunction with our partners at the Government Printing Office, we currently have a Request for Proposals out to the industry. We expect to award a contract for the purchase of integrated circuits and the associated antenna array later this summer. We also expect to produce our first operational biometric passports this December at the Special Issuance Facility here in Washington. Our first biometric passports produced will be "official and diplomatic" passports, used by USG employees, in order to minimize problems for the general public should there be any production problems. We plan to begin producing biometric tourist passports in February 2005 at our passport agency in Los Angeles. These books will then be used as part of a multi-nation interoperability test that will be undertaken by our colleagues from DHS and their counterparts from other governments such as Australia and New Zealand that will by then also produce passports with embedded biometrics. We hope to be in full production at all 16 passport facilities by December 2005.

Should the current October 26, 2004 deadline not be extended, we anticipate a significant adverse impact on Department operations overseas. Since travelers from VWP countries with passports issued on or after October 26, 2004 without biometrics will need visas to travel to the United States, we estimate that the demand for non-immigrant visas will jump by over 5 million applications in FY 2005. This represents a 70% increase in our nonimmigrant visa workload. There are no easy solutions to handling this tremendous increase in our workload. True, this is a temporary problem because the workload will progressively decrease as VWP countries begin mass production of biometric passports. But in the interim, we would need to implement plans for a massive surge in visa processing, which would involve extra expense, diversion of personnel from other vital functions, and extending service hours, perhaps even to around-the-clock 24/7 visa processing at some posts. Even with a "Manhattan Project" approach, we cannot be sure that we could meet the demand without creating backlogs and long waits for appointments. We are already working hard on public diplomacy outreach to address some of the negative perceptions and misunderstandings concerning tightened U.S. visa policies. Even longer wait times would make it even more difficult to convince people worldwide that America welcomes and values their presence. The delays resulting from this increased nonimmigrant visa demand will also discourage travel to the U.S. as visitors, both tourist and business people, may "vote with their feet" and choose to travel and take their business elsewhere, or defer their travel to the U.S., hurting relations with some of our closest friends and allies, and harming the American economy.

Although we are confident that VWP Countries can meet the October 2006 requirement based on prior representations and information provided by all VWP countries, we know that many will not be able to meet this requirement before then. A one-year extension is not sufficient. At the same time that we, along with the VWP countries, work to expeditiously get our biometrically enabled passport plans in place, we are also not slowing down on any of our other travel security enhancements. Extending

the deadline to make sure all countries get it right the first time is only part of our answer. So is advanced passenger screening, and so is increased sharing of lost and stolen passport information, as we have already done with INTERPOL, and which we will press other nations to do. On the diplomatic front, we will continue to pursue vigorous efforts at the highest levels to ensure that the VWP countries remain committed to introducing biometric passports as quickly as possible. Senior Department officials have and will continue to use every opportunity in regularly scheduled meetings with officials from the European Union, the G-8 and the Asia-Pacific Economic Commission to challenge other governments to act aggressively. This issue will be a top priority at all VWP Embassy sections, not just the consular section. As we develop our own passport program we will continue to share what we have learned with others in groups such as the G-8, on the margins of international conferences, and in bilateral exchanges. And we will continue to monitor each country's progress, continue to press for rapid action and enhance our efforts for increased data sharing with the VWP countries.

We are also asking every VWP country to monitor their progress in meeting the requirements of the legislation. We will thus be able to coordinate at both the political as well as operational level. Among the benchmarks for progress, we will review whether each country has:

- Identified a project manager to be the primary operational point of contact;
- Established a time line for compliance with the program;
- Developed a procurement approach, including purchase of chips, and;
- Established a pilot project to test configuration, durability, operability.

In addition, DHS with Department of State participation is conducting VWP country biennial reviews over the next few months. The schedule for these reviews is ambitious; in-country visits began in mid-May. Interagency teams comprising four to six members will travel for two to three week periods to several countries at a time. The assessment teams are collecting information from host government officials on a comprehensive list of issues such as lost and stolen passports, the naturalization process, revocations of passports, crime statistics, and local laws pertaining to country police policies. These teams are also addressing law enforcement and data sharing cooperation with the U.S. government. All visits will be completed by July 15.

We will take every opportunity during the course of these visits to remind governments of the importance of introducing biometrics into their passports as soon as technically feasible. We will ensure that they all understand that if they fail to meet the extended deadline, we will have no alternative but to begin requiring visas for travelers from those countries. Further, to continue to tighten our security posture, DHS announced in April that beginning September 30, 2004, it will enroll all VWP travelers in US-VISIT – the program that will track the entry and exit of foreign visitors by using electronically scanned fingerprints and photographs.

The inclusion of biometrics in international travel documents is an important step in continuing to improve our ability to verify the identity of prospective travelers to the

United States, especially individuals who might be terrorists, criminals, or other aliens who present a security risk to the United States. The Department of State is working hand in hand with our colleagues at DHS to facilitate legitimate international travelers and to prevent those who pose a threat from entering our country. We are also working with the VWP countries to deploy biometrically enabled passports that enhance the security of travel documents and the safety of international travelers. Ensuring the security of our borders and our nation is our number one priority. That is why we need the additional time to get it right the first time. Thank you.

News Release

JUDICIARY COMMITTEE

United States Senate • Senator Orrin Hatch, Chairman

June 15, 2004 Contact: Margarita Tapia, 202/224-5225

Statement of Chairman Orrin G. Hatch
Before the United States Senate Committee on the Judiciary
Hearing on

"BIOMETRIC PASSPORTS"

Good morning and welcome to the hearing on biometric passports. Since last fall, this Committee has held eight oversight hearings that substantially focus on our Nation's efforts to prevent and respond to terrorism on American soil. The purpose of these hearings is to make sure that the United States government is taking every possible step to protect this country and its citizens from the evil intentions of terrorists, and that every available resource is focused toward that end. Implementation of the biometric passport program will be an important resource in our fight against terrorism, and we should be vigilant in our efforts to fully implement the program.

Today, we focus our attention on the biometric passport requirement set out in the "Enhanced Border Security and Visa Entry Reform Act." This legislation provided crucial tools to tighten immigration procedures and close loopholes in our border security which were, in my view, of paramount importance after the catastrophic attacks this Nation suffered on September the 11th, 2001. I was proud to be an original cosponsor of this legislation, and am disappointed that more than two years after its enactment, we are faced with the reality that the biometric passport deadline of October 26, 2004 will not be met.

Now, I understand that when we called for the development and inclusion of biometric passports, the fundamental technologies were not yet mature. Nonetheless, many of us believed that we needed cutting-edge technology in order to thwart the increasingly sophisticated terrorists. This mandate has presented difficult challenges for the many capable scientists and technicians who have dedicated themselves to this effort. But we can – and must – demand that the countries who participate in the Visa Waiver Program begin producing and distributing these passports. Every day that biometric identifiers are not utilized, our country and its citizens are more vulnerable to terrorist attacks. I strongly urge the Department of State and Department of Homeland Security to work with these participating countries in the upcoming months to establish an interoperable system for biometric passports.

I have spoken to Secretary of State Powell concerning the importance of the biometric passport issue, and during his testimony before this Committee last week,

Secretary Ridge also emphasized the importance of this issue. Both of these men, whom I highly respect, have requested a two-year extension to the current biometric passport deadline of October 26th, 2004. However, I am concerned with the national security implications that such a lengthy extension may cause. Frankly, I would like to inquire why a one-year extension is not feasible for implementation of the biometric passport program. As this deadline extension has implications on our national security, I hope that our witnesses today can fully explain to this Committee the reasons for extending the current biometric passport deadline.

Today, the Committee will hear from two panels of witness testimony. The first panel consists of testimony by the Honorable Maria Cantwell, Senator from the state of Washington. I would like to welcome Senator Cantwell, who was a cosponsor of the Enhanced Border Security and Visa Entry Reform Act. I know that she feels strongly about this issue, and I thank her for taking the time to appear before the Committee.

The second panel consists of testimony by the Honorable Asa Hutchinson, Under Secretary for Border and Transportation Security at the Department of Homeland Security, and the Honorable Maura Harty, Assistant Secretary for Consular Affairs at the Department of State. I welcome them to the Committee, and appreciate their testimony on this important issue of national security.

###

TESTIMONY OF
ASA HUTCHINSON, UNDERSECRETARY
BORDER AND TRANSPORTION SECURITY
DEPARTMENT OF HOMELAND SECURITY
BEFORE THE SENATE COMMITTEE ON THE JUDICIARY
June 15, 2004

Chairman Hatch and other distinguished Members, it is a pleasure to appear before you today to discuss the necessity to extend the Visa Waiver Program (VWP) countries[1] requirement to produce International Civil Aviation Organization (ICAO) compliant, biometric passports for two years and the corresponding requirement for the Department of Homeland Security (DHS) to install equipment and software at all Ports-of-Entry (POEs) to allow biometric comparison and authentication of those passports.

I. Statutory Requirements in Enhanced Border Security Act

The VWP enables citizens of certain countries to travel to the United States for tourism or business for ninety days or less without obtaining a visa. While visa-less travel encourages travel and trade with our allies, it also makes the program attractive to those wishing to avoid visa security checks conducted at U.S. consulates abroad. To help address this security vulnerability, the Enhanced Border Security and Visa Reform Act (EBSA) requires that beginning on October 26, 2004, VWP countries have a program in place to issue their nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with ICAO standards as a condition of continued participation in the VWP program. The law also requires 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.

While most VWP program countries will be able to certify that they have a program in place to issue biometric passports by the October deadline, very few, if any, VWP countries will actually be able to begin issuing biometric passports by that date. The result is that millions of visitors from VWP countries who are issued non-ICAO compliant passports after October 26, 2004, will be required to obtain visas prior to traveling to the United States. The issue is not a lack of will or commitment to achieving the standard by these countries, but rather challenging scientific and technical issues.

ICAO adopted high-level technical standards for biometric passports in May 2004. These standards provided for the inclusion of a full-face image on a contactless chip as well as

[1] The following 27 countries are currently in the VWP: Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom (which includes citizens with the unrestricted right of permanent abode in England, Scotland, Wales, Northern Ireland, the Channel Islands and the Isle of Man).

minimum chip storage capacity, security standards, and technical benchmarks. However, the ICAO specifications for biometrics in passports are just the start of the process. The international community, both public and private sectors, are moving this process forward. The standards for facial recognition data storage and exchange process of the International Standards Organization (ISO) have been incorporated into the biometric passport standards adopted by the ICAO. This will ensure that the digital photographs stored on biometric passports are of the optimum quality and conform to the best practices for facial recognition systems.

On June 17 in London, the ICAO e-Passports Task Force will meet to provide detailed specifications and clarification of international standards to ensure that global interoperability can be achieved. This is to enable manufacturers of readers and writers to refine their hardware and software prior to undergoing any further pilots or testing.

The U.S. is working with Australia, New Zealand, Germany, the United Kingdom, the Netherlands, Japan, and potentially Belgium on a joint testing project where the digital images stored on passports will be compared against live images. This will involve tests in both laboratory settings and in a controlled test situation at ports of entry.

For challenging technical reasons, DHS is also not currently in a position to acquire and deploy equipment and software to biometrically compare and authenticate these documents. DHS cannot today acquire one reader that will be able to read all chips utilized in the ICAO compliant biometric passports. However, we believe that by the fall of 2006, the technology required to implement successfully a security system based on the ICAO standards will be evolved and we will then be able to fully implement the international biometric standard required by the EBSA.

Acknowledging the current state of technology, and the potential for harm to our international relations with our closest allies, DHS and DOS have requested that the October 26, 2004, deadline be extended to November 30, 2006, for those sections of the EBSA relating to the production of ICAO-compliant biometric passports, and deployment of equipment and software to read them.

Based on the information provided to us by these countries on their status and their expected implementation dates, as well as DOS's own experience as it moves to implement this standard for U.S. Passports, we believe that all countries will be compliant by the November 30, 2006, deadline.

II. Increasing Security through US-VISIT Expansion

While we recognize the need to extend the date for these new processes, we are focused on the need to continue to increase security at the borders. Therefore, DHS has announced that we will begin expanding US-VISIT procedures to VWP visitors beginning on September 30, 2004. Enrolling VWP passengers in US-VISIT will begin at air and sea ports of entry on September 30 and be phased in at the land borders in accordance with US-VISIT's deployment schedule mandated by statute.[2]

In FY 2003, DHS recorded the admission of approximately 13 million VWP travelers through air and sea POEs. This number includes multiple visits to the U.S. by a single individual. By expanding US-VISIT to include processing of VWP travelers, DHS will double the number of admissions processed through US-VISIT from its current status. As discussed below, we are confident that the US-VISIT infrastructure can continue to function quickly and accurately after the expansion. In addition, while the number of VWP travelers arriving at land ports of entry is small, the expansion rollout plan will allow for biometric enrollment for those travelers as well.

DHS believes that processing visitors traveling under VWP in US-VISIT achieves several important security objectives. These security objectives include:

- Conducting appropriate security checks: We will conduct checks of VWP visitors against appropriate lookout databases available to inspectors, adding additional biometric-based checks available through US-VISIT.
- Freezing identity of traveler: We will biometrically enroll visitors in US-VISIT – freezing the identity of the traveler and tying that identity to the travel document presented.
- Matching traveler identity and document: We will biometrically match that identity and document if a traveler returns to the United States, enabling the inspector to determine whether the traveler complied with the terms of his or her previous admission and is using the same identity.
- Documenting arrival and departure: We will collect automated arrival and departure information on travelers. We will update their record to reflect changes in their immigration status while they are in the U.S.
- Determining overstays: We will use collected information to determine whether individuals have overstayed the terms of their admission. This information will be used to determine whether an individual should be apprehended or whether the individual should be allowed to enter the U.S. upon his or her next visit.

The VWP countries have been supportive of this change. Response to our announcement of this change from VWP countries has been positive. These countries appreciate both the U.S. interest in increasing security, and our support for an extension to the ICAO compliant biometric passport requirement. Although the majority of travelers from VWP countries are exempt from

[2] US-VISIT will be deployed to the 50 busiest land border ports of entry by December 31, 2004 and to the rest of land border ports of entry by December 31, 2005. The Immigration and Naturalization Service Data Management Improvement Act (DMIA) of 2000 established a series of deadlines for the implementation a data system that would record arrival and departure information on non-United States Citizens.

the requirement to obtain a nonimmigrant visa, those who are required to obtain one are already successfully processed through US-VISIT. Since the implementation of US-VISIT through June 8, 2004, approximately 600,000 VWP nationals with visas have been processed through US-VISIT.

Many of the VWP countries themselves are actively engaged in developing programs like US-VISIT that allow them to collect biometrics through the visa issuance process and match those biometrics upon entry into the country. We are actively working with many of these countries to share information about terrorism, other security threats, and opportunities for improvements in immigration and border management.

In order to expand US-VISIT to VWP travelers, DHS will have to implement both technical and procedural changes. In terms of technical changes, DHS is investing in additional hardware and software, including additional biometric matchers, database capacity, processing power, and backup/storage capability, that will support the additional volume and maintain the response times needed on biometric watch list checks and identity matching. DHS is also modifying processing procedures and making other operating environment changes to accommodate the increase. These changes will vary in scope, depending on the volume of VWP travelers at that location.

III. US-VISIT IMPLEMENTATION AND SUCCESS TO DATE

DHS has established US-VISIT to achieve the following goals:

- Enhance the safety of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of travelers to the United States.

US-VISIT is a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. Using biometrics such as digital, inkless fingerscans and digital photographs, DHS is able to determine whether the person applying for entry to the United States is the same person who was issued the visa by DOS. Additionally, DOS and DHS use biometric and biographic data to check against appropriate lookout data, improving DOS's ability to make visa determinations and DHS's ability to make admissibility decisions at entry.

US-VISIT procedures are clear, simple, and fast for visitors.

DHS deployed the first increment of US-VISIT on time, within budget, and has exceeded the mandate established by Congress as it includes biometrics ahead of schedule. On January 5, 2004, US-VISIT entry procedures were operational at 115 airports (covering 99% of air travelers who use visas to enter the United States) and 14 seaports. As of June 8, more than 5 million foreign visitors have been processed under the US-VISIT entry procedures. In addition, we began pilot testing biometric exit procedures at one airport and one seaport.

Already US-VISIT has matched over 579 persons against criminal databases and prevented more than 196 known or suspected criminals from entering the country. In addition, four hundred and seventy-nine people were matched while applying for a visa at a State Department post overseas.

Our border management system impacts the security of our citizens and our visitors, affects billions of dollars in trade and travel and helps define relations with our international partners. There is a need to improve this system and bring it into the 21st century with a new integrated system of technological processes that will keep our country's economic and national security strong. This 21st century technology will provide an important step toward achieving the President's goal of secure U.S. borders.

We respect our visitors' privacy and seek to enable them to pass through inspection quickly so they can enjoy their visit in our country. However, as people attempt to enter the United States, we must know who they are and whether they intend to do us harm. The ability of US-VISIT to rapidly screen applicants' biometrics and biographic information through watch lists and databases means we can have security and control without impeding legitimate travelers, and we can also help protect our welcomed visitors by drastically reducing the possibility of identity theft. Moreover, as visitors leave the country, we must know that they have not overstayed the terms of their admission.

US-VISIT will be rolled out in increments to ensure that the foundation is strong and the building blocks are effective. With the deployment of the entry components at air and seaports, we have made a strong beginning. We are on track to meet the December 31, 2004, deadline to integrate US-VISIT procedures at the 50 busiest land border ports of entry.

US-VISIT is dedicated to safeguarding the privacy of traveler information. US-VISIT has extended the principles of the 1974 Privacy Act[3] to all individuals processed through the program – even though the law only applies to U.S. Citizens and Lawful Permanent Residents. US-VISIT has implemented a privacy program that includes a privacy policy[4] and a three-stage process for redress,[5] if individuals have concerns about their information.

---

[3] The principles and protections of the Privacy Act are centered around notice to those who will be subject to information collection; notice of how the information will be used and how long it will be retained; and adherence to those uses.

[4] The US-VISIT Privacy Policy and Privacy Impact Assessment (PIA) can be found at: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0333.xml

[5] US-VISIT has implemented a three-stage process for redress if an individual has a concern. If an affected individual requests a change or when a DHS Officer determines that an inaccuracy exists in the individual's record, the DHS Officer can modify the record. If an individual is not satisfied with this response, he or she can contact the US-VISIT Privacy Officer and ask for assistance. The individual can request a review by the DHS Privacy Officer, to address any remaining concerns.

A. *Moving to a "Virtual Border" Solution*

The vision of US-VISIT is to deploy an end-to-end border management program. This comprehensive view of border management leads to a virtual border. It elevates the requirement to develop the best processes to manage data on visitors. It will provide information to the immigration and border management decision makers to support the pre-entry, entry, status management, exit and analysis processes.

Much of the emphasis to date has focused specifically on the entry and exit processes at the ports of entry – the "port-centric" solution. One of the key initiatives of the US-VISIT program is to adjust this focus to a "virtual border" solution, placing equal emphasis on the pre-entry, entry, status management, exit, and analysis processes associated with this Program. The virtual border will enhance national security by matching the identity of visitors, facilitate legitimate trade and travel, and ensure the integrity of our immigration system by improving enforcement.

1. Pre-Entry

For millions of visitors, entry into the United States must be preceded by the issuance of travel documents at a U.S. embassy or consulate abroad. The purpose of the pre-entry process is to determine eligibility for immigration status and/or visas at DOS consular offices worldwide or DHS Service Centers.

The pre-entry process is a critical component of the US-VISIT virtual border. The consular officers gather a large amount of information prior to a visitor's arrival at a port. This data is now available to appropriate border management agencies. In turn, the US-VISIT Program can provide additional information about the individual, including a history of prior entries and exits, biometrics, or prior immigration status information, that can be used to match identity or search watch lists to the consular officer or Citizenship and Immigration Services adjudicator who is determining a visitor's eligibility.

Since the beginning of 2004, the pre-entry process includes analysis of the manifest supplied by the airlines for each international flight to determine the nonimmigrant visa holders on board the plane. This is done through the Advanced Passenger Information System (APIS). The U.S. Customs and Border Protection Officers analyze this information to know in advance whether a visitor may require additional review at inspection.

2. Entry Process

The purpose of the entry process is to determine the admissibility of visitors requesting entry into the United States at air, land, or seaports. The entry process can begin at a primary port inspection booth at an air, sea, or land ports, or at a temporary inspection location such as a ship lounge. Visitors can also be inspected at certain pre-inspection locations overseas, such as Shannon Airport in Ireland.

As part of the US-VISIT entry process, visitors will be required to provide biometric data, biographic data, and/or other documentation. This data is used to match identity, determine

proper visa classification, and to query the watch list. Inspectors match identity of each visitor collected by DOS and determine the visitor's admissibility.

All ports share similarities in the inspection processes. Inspectors must quickly conduct a primary inspection and determine if the applicant should be recommended for a more in-depth review at the secondary inspection point. The average primary inspection of U.S. citizens, lawful permanent residents, and visitors, lasts approximately one minute.

Although all inspections involve certain basic tasks, there are marked differences between an inspection conducted at an air or sea port and one conducted at a land port because of the different physical environment and different travel patterns.

To expedite the flow of traffic at land ports, DHS has implemented several programs, such as the Secure Electronic Network for Traveler's Rapid Inspection (SENTRI) or Dedicated Commuter Lane, and NEXUS, using Radio Frequency (RF) technologies to be able to preposition and collect information for inspection. For land borders, we are considering expanded use of RF technology to expedite processing of frequent border crossers using biographical data as part of the virtual border solution.

3. Status Management Includes Identifying Overstays

Managing the status of visitors once inside the borders of the United States includes, but is not limited to:

- Ensuring that determinations relating to a visitor's legal extension of stay or change of immigration status are informed by previous determinations by State at visa issuance, DHS when the individual was admitted, or the individual's compliance on previous visits to the United States.
- Updating an individual's admission record to reflect changes in immigration status or extensions of their period of admission.
- Matching arrival and departure records to determine if individuals have overstayed the terms of their admission.
- Identifying violations of terms of admission.
- Referring lookout or other information demonstrating an individual's failure to comply with his or her immigration status to agencies and organizations responsible for enforcement.

Maintaining the status of visitors while in the United States is an integral part of border management and ensures the integrity of the immigration system. One of the US-VISIT Program's primary roles in status management will be the overstay calculation, and exchanging appropriate entry and exit information with case management systems, especially those managed by U.S. Citizenship and Immigration Services.

4. The Exit Process Will Capture Departure Information

Currently, our exit procedures are based upon departure information from passenger manifests shared with us by carriers. We match this information with the admission information and identify those likely to have overstayed the terms of their admission. Our goal is to enhance our

ability to match arrivals and departures by using biometrics. We are testing this with various pilot programs, one of them being at the Baltimore-Washington International Airport. We plan to expand our pilot program to a total of 15 air and seaports over the next several months. We will pilot test three options and evaluate the results to identify the best, most efficient and effective process. These pilot programs will build on the current kiosk pilot and test mobile devices.

5. The Analysis of Information

The purpose of the analysis process is to provide information that will aid immigration and border management officials in their decision-making process. Currently, the Arrival/Departure Information System (ADIS) system is the primary data source for use in these analyses.

One of the activities conducted in the analysis process is the determination of those who have overstayed the terms of their admission. Each week, the Immigration and Customs Enforcement (ICE) Compliance Enforcement Unit (CEU) receives a report of those individuals for whom the period of admission has expired and no departure record has been received. The ICE/CEU evaluates these records, determines whether additional information may exist that would indicate that the person has departed timely or is in a status that would result in their continued presence within the U.S., and then acts on the remaining cases appropriately.

A visitor's information is stored and routinely updated in ADIS. Information compiled in ADIS will tell the officer if an individual has complied with the terms of his or her admission. If the traveler's history illustrates immigration violations, the officer would use that information to inform his or her decision.

As the US-VISIT program evolves, this process will take on an ever-increasing level of importance. Emphasis will be placed on providing an increased level of information to all border management personnel (e.g., the consular official, the inspector, the adjudicator, and the investigative officer) to aid them in making critical decisions.

6. Watch Lists

At various points in the pre-entry, entry, status management, and analysis processes, decision makers are supported by systems checks against data consolidated from law enforcement and intelligence sources that identify persons of interest for various violations.

All names and fingerscans are checked against watch lists to identify known or suspected terrorists, criminals, and immigration violators. Terrorist watch list checks are coordinated with the Terrorist Screening Center (TSC).

B. *The Success Stories of US-VISIT*

Through the US-VISIT biometric process, DHS and DOS have identified many individuals who are the subjects of lookout records. These included rapists, drug traffickers, and those who have committed immigration offenses or visa fraud.

Here are details of a few examples.

- Interception of Drug Trafficker who escaped from Prison – On January 14, 2004, at Miami International Airport, a man was identified as wanted by the U.S. Marshals for escaping from La Tuna Federal Correction Facility where he had been serving a sentence for a conviction of dealing cocaine. The individual was turned over to the U.S. Marshals.

- Visa Fraud Uncovered – On January 14, 2004, Customs and Border Protection determined that a woman was trying to enter the United States using a false name, after determining that the woman was not the same individual whose visa photo appeared in the database. The traveler was a woman who had been arrested in April 2000 in New Orleans, convicted of passport fraud, placed on 5 years probation, and prohibited from entering the United States during that time. The woman was removed from the United States after it was determined that she did not meet the guidelines for criminal prosecution.

- Convicted Sexual Offender Identified – In New York City, on February 19, 2004, US-VISIT identified an individual who had a prior conviction for having sex with a minor in 2000, was registered as a convicted sex offender, and was removed from the United States in 2001 as an aggravated felon. He was given an expedited removal and a 20-year ban on re-entry after it was determined that he did not meet the guidelines for criminal prosecution.

- Rape Suspect Caught - On February 22, 2004, at Miami International Airport, biographic and US-VISIT biometric checks alerted officers to an active warrant from New York City for rape. Criminal history checks also uncovered 3 prior convictions for possession or sale of marijuana in 1994 and 1995, as well as a 1998 rape arrest. He was turned over to Miami-Dade police for extradition to New York.

US-VISIT is critical to our national security as well as our economic security, and its implementation is already making a significant contribution to the efforts of DHS to provide a safer and more secure America. We recognize that we have a long way still to go. We will build upon the initial framework and solid foundation to ensure that we continue to meet our goals to enhance the security of our citizens and visitors while facilitating travel for the millions of visitors we welcome each year.

We want to emphasize that we continue to be a welcoming nation, a nation that invites visitors to study, do business, and enjoy our country. We also owe it to our citizens and visitors to deny entry to persons wishing to do harm to the United States.

We are committed to building a program that enhances the integrity of our immigration system by catching the few and expediting the many, the United States is leading the way in this new era – keeping our doors open and our nation secure.

IV. Conclusion

Countries in the VWP are our closest allies and economic partners. Seeking a two-year extension of the October 26, 2004 biometric deadline permits citizens of our allies to travel to the United States without undue burden or delay, while processing VWP travelers through US-VISIT allows DHS to achieve our security objective and facilitate the flow of legitimate travelers.

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

Statement of Senator Patrick Leahy,
Ranking Member, Senate Judiciary Committee
Hearing on "Biometric Passports"
June 15, 2004

Today, we welcome back Senator Cantwell, whose leadership in this Committee on securing our borders and our nation is very much missed. I am pleased that she remains involved in these issues and continues to contribute to our national security, and I look forward to her testimony. We will then hear from Undersecretary Hutchinson, a frequent guest of this Committee, and Assistant Secretary of State Maura Harty. Each of our witnesses will assist us as we consider whether to extend the congressionally mandated October deadline for nations that participate in the visa waiver program to provide passports with biometric identifiers to their citizens. The visa waiver program allows nationals of 27 countries to travel to the United States for up to 90 days with only a passport, rather than a visa.

This is a program that has substantial economic benefits for our nation. Naturally, after the September 11 attacks, Congress took understandable measures to place safeguards within the program to limit its use to law-abiding travelers. One of those safeguards was to require participating nations to adopt high-technology passports – just as we are developing biometric passports ourselves. We placed a deadline of Oct. 26, 2004, for the adoption of such passports, but very few of the 27 visa waiver nations will meet that deadline. These nations are not alone, as our own adoption of biometric passports is not expected to take place until the end of 2005.

Congress must now choose either to maintain or extend the Oct. 26 deadline. If we maintain it, travelers from Britain, Australia, Germany and other U.S. allies will have to go to U.S. consular offices abroad and obtain visas to come here. This will create a substantial burden on the State Department, one the Department tells us it could not meet even if its existing consular officers worked for 24 hours a day, seven days a week. If we do not extend the deadline, we will assuredly see a reduction in foreign travel here. This would greatly harm our economy, particularly affecting those tourism-dependent industries that are already struggling to recover from the financial damage caused by the Republican leadership's failure to pass bipartisan legislation to expand the number of H-2B visas available for the temporary foreign workers on which those industries rely.

If we extend the deadline, we will have to be vigilant about protecting our security. I am pleased that the Department of Homeland Security will be including travelers from visa waiver countries in the US VISIT program, which records the entry and exit of foreign visitors. In addition, the U.S. receives passenger manifests for planes arriving in the

country, providing our security personnel with the opportunity to review the backgrounds of visitors traveling without visas before they are ever allowed entry to this country. I think these developments will help alleviate the reasonable security concerns that have been expressed about the continuation of the visa waiver program in its current form.

I do have some technology concerns that I hope our witnesses today, and the Administration as a whole, will consider. One concern is the way biometric information will be stored on the chip. It is my understanding that an encrypted version of the entire images, rather than encrypted data based on features of the biometric, will be included on the chip in order to allow additional flexibility in choosing standards at a later time. However, should this system be compromised or hacked -- particularly by an insider or contractor -- these entire images could become compromised, possibly risking many future uses of this important technology. We should consider whether it would be better to take additional time to finalize the standards issue rather than to include entire images on the chip.

I am also concerned that the process for setting the technology, standards and privacy protections for the biometric passports is occurring largely outside of congressional and public view, in negotiations by U.S. representatives and others in the International Civil Aviation Organization. This process could have significant impact on U.S. domestic policy and we should keep this in mind as these efforts progress. To the extent that this process results in other nations collecting information on U.S. citizens, we should ensure that Americans' personal information receives the same kind of protection abroad that it would receive here.

While discussing privacy issues, I would also like to raise the issue of facial recognition technology. While I understand that the first generation of the biometric passport system will not utilize such technology, the prospect of its future use raises many questions that we as a Congress would need to consider. We would need to understand both the timetable and costs of such a program, and the precautions and safeguards that would be in place to protect privacy and security.

So as we convene this hearing, I am sympathetic to the need to extend this deadline, and I look forward to reviewing the testimony of our witnesses.

# # # # #

○